

日 本 国 特 許 庁
JAPAN PATENT OFFICE

07.01.2005

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2 0 0 4 年 4 月 1 9 日

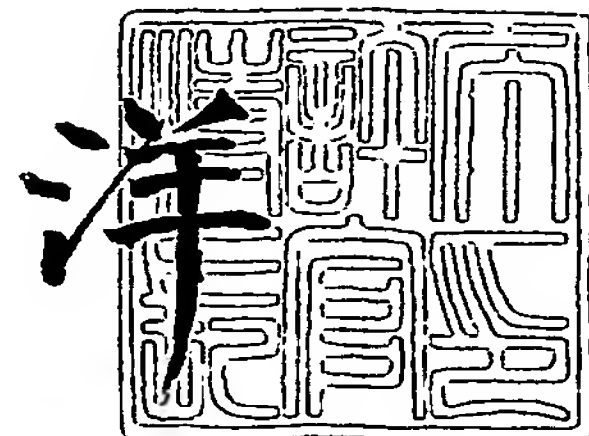
出 願 番 号
Application Number: 特 願 2 0 0 4 - 1 2 2 5 2 4
[ST. 10/C]: [J P 2 0 0 4 - 1 2 2 5 2 4]

出 願 人
Applicant(s): ソニー株式会社

2 0 0 4 年 1 2 月 2 4 日

特許庁長官
Commissioner,
Japan Patent Office

小 川



【書類名】 特許願
【整理番号】 0490031904
【提出日】 平成16年 4月19日
【あて先】 特許庁長官殿
【国際特許分類】 H04N . 5/91
【発明者】
 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内
 【氏名】 木谷 聡
【特許出願人】
 【識別番号】 000002185
 【氏名又は名称】 ソニー株式会社
【代理人】
 【識別番号】 100082131
 【弁理士】
 【氏名又は名称】 稲本 義雄
 【電話番号】 03-3369-6479
【先の出願に基づく優先権主張】
 【出願番号】 特願2004- 4798
 【出願日】 平成16年 1月 9日
【手数料の表示】
 【予納台帳番号】 032089
 【納付金額】 16,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9708842

【書類名】 特許請求の範囲**【請求項 1】**

データの転送を制御する転送制御手段と、
前記転送制御手段が前記データの転送を制御した回数をカウントするカウント手段と、
前記カウント手段によりカウントされた回数が、所定の閾値以上になったか否かを判断する第 1 の判断手段と、
前記第 1 の判断手段により前記回数が前記閾値以上になったと判断された場合、前記転送制御手段に、前記データの転送を停止するように指示を出す第 1 の指示手段と、
前記転送制御手段により転送が制御される前記データの暗号化または復号に用いられる初期ベクトルを生成する生成手段と、
前記転送制御手段により転送が制御される前記データを授受する他の装置から、前記初期ベクトルの供給が指示されたか否かを判断する第 2 の判断手段と、
前記第 2 の判断手段により前記初期ベクトルの供給が指示されたと判断された場合、前記生成手段に前記初期ベクトルの生成を指示するとともに、前記カウント手段によりカウントされている前記回数をリセットするように指示を出す第 2 の指示手段と
を備えることを特徴とする情報処理装置。

【請求項 2】

前記第 1 の指示手段による指示が出された場合、前記他の装置に対して前記データの転送が停止されたことを示すメッセージを出力する出力手段を
さらに備えることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】

データの転送を制御する転送制御ステップと、
前記転送制御ステップの処理で前記データの転送が制御された回数をカウントするカウントステップと、
前記カウントステップの処理によりカウントされた回数が、所定の閾値以上になったか否かを判断する第 1 の判断ステップと、
前記第 1 の判断ステップの処理で前記回数が前記閾値以上になったと判断された場合、前記転送制御ステップにおける処理で、前記データの転送が停止されるように指示を出す第 1 の指示ステップと、
前記転送制御ステップの処理で転送が制御される前記データの暗号化または復号に用いられる初期ベクトルを生成する生成ステップと、
前記転送制御ステップの処理で転送が制御される前記データを授受する他の装置から、前記初期ベクトルの供給が指示されたか否かを判断する第 2 の判断ステップと、
前記第 2 の判断ステップの処理で前記初期ベクトルの供給が指示されたと判断された場合、前記生成ステップによる処理で前記初期ベクトルが生成されるように指示するとともに、前記カウントステップの処理によりカウントされている前記回数がリセットされるように指示を出す第 2 の指示ステップと
を含むことを特徴とする情報処理方法。

【請求項 4】

データの転送を制御する転送制御ステップと、
前記転送制御ステップの処理で前記データの転送が制御された回数をカウントするカウントステップと、
前記カウントステップの処理によりカウントされた回数が、所定の閾値以上になったか否かを判断する第 1 の判断ステップと、
前記第 1 の判断ステップの処理で前記回数が前記閾値以上になったと判断された場合、前記転送制御ステップにおける処理で、前記データの転送が停止されるように指示を出す第 1 の指示ステップと、
前記転送制御ステップの処理で転送が制御される前記データの暗号化または復号に用いられる初期ベクトルを生成する生成ステップと、
前記転送制御ステップの処理で転送が制御される前記データを授受する他の装置から、

前記初期ベクトルの供給が指示されたか否かを判断する第 2 の判断ステップと、

前記第 2 の判断ステップの処理で前記初期ベクトルの供給が指示されたと判断された場合、前記生成ステップによる処理で前記初期ベクトルが生成されるように指示するとともに、前記カウンタステップの処理によりカウントされている前記回数がリセットされるように指示を出す第 2 の指示ステップと

を含む処理をコンピュータに実行させることを特徴とするプログラム。

【請求項 5】

データの転送を制御する転送制御ステップと、

前記転送制御ステップの処理で前記データの転送が制御された回数をカウントするカウントステップと、

前記カウントステップの処理によりカウントされた回数が、所定の閾値以上になったか否かを判断する第 1 の判断ステップと、

前記第 1 の判断ステップの処理で前記回数が前記閾値以上になったと判断された場合、前記転送制御ステップにおける処理で、前記データの転送が停止されるように指示を出す第 1 の指示ステップと、

前記転送制御ステップの処理で転送が制御される前記データの暗号化または復号に用いられる初期ベクトルを生成する生成ステップと、

前記転送制御ステップの処理で転送が制御される前記データを授受する他の装置から、前記初期ベクトルの供給が指示されたか否かを判断する第 2 の判断ステップと、

前記第 2 の判断ステップの処理で前記初期ベクトルの供給が指示されたと判断された場合、前記生成ステップによる処理で前記初期ベクトルが生成されるように指示するとともに、前記カウンタステップの処理によりカウントされている前記回数がリセットされるように指示を出す第 2 の指示ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【書類名】 明細書

【発明の名称】 情報処理装置および方法、プログラム、並びに記録媒体

【技術分野】

【0001】

本発明は、情報処理装置および方法、プログラム、並びに記録媒体に関し、特に、暗号化に関わる処理を実行する際に用いて好適な情報処理装置および方法、プログラム、並びに記録媒体に関する。

【背景技術】

【0002】

さまざまな装置で、デジタルデータを授受することが一般的になりつつあるが、デジタルデータは、不正に利用されても、その質（例えば、画質や音質）が劣化しないため、不正に利用されないための対策が必要とされる。（例えば、特許文献1参照）

【0003】

また近年普及しつつあるDVD（Digital Versatile Disc）等の記録媒体では、1枚の記録媒体（ディスク）に、例えば映画1本分の大量のデータをデジタル情報として記録することが可能である。このように映像情報等をデジタル情報として記録することが可能となると、不正なコピーを防止して著作権者の保護を図ることが益々重要になってくる。

【0004】

そこで、例えば、DVDにビデオコンテンツを格納したDVDビデオでは、著作権保護技術として、CSS（Content Scramble System）方式が採用されている。図1は、CSS方式を用いて暗号化されたデータが記録されている記録媒体と、その記録媒体を再生する装置の構成の一例を示す図である。

【0005】

図1においては、記録媒体として、ディスク11を例に挙げて図示してある。ディスク11には、ディスク11を識別するためのディスクキー（Secured Disc Key）21、記録されているデータの所定の単位毎に設けられているタイトルキー（Encrypted Title Key）22、および、データ（Scrambled Data）23が記録されている。タイトルキー22は、例えば、ディスク11に映画が記録されているような場合、チャプター（Chapter）毎に設けられる。

【0006】

ディスクキー21とタイトルキー22は、暗号化された状態（または、容易に読み出すことが（盗用することが）できない状態）でディスク11に記録されている。また、データ23は、タイトルキー22を用いたスクランブル（Scramble）がかけられた状態でディスク11に記録されている。

【0007】

プレーヤ12は、ディスク11に記録されているキーやデータを読み出すことにより、データ23の再生を行う。プレーヤ23は、復号（Decrypt）部32、復号部33、デスクランブル（DeScramble）部34、および、デコーダ（Decoder）35を有する構成とされている。また、プレーヤ12は、マスタキー（Master Key）31を管理する管理部（不図示）も有している。

【0008】

復号部32は、ディスク11から読み出されたディスクキー21を、マスタキー31を用いて復号し、その復号したディスクキー21を復号部33に供給する。復号部33には、ディスク11から読み出されたタイトルキー22も供給される。復号部33は、復号されたディスクキー21により、暗号化されているタイトルキー22を復号する。復号されたタイトルキー22は、デスクランブル部34に供給される。デスクランブル部34には、ディスク11から読み出されたデータ23も供給される。

【0009】

ディスク11から読み出され、プレーヤ12に供給されるデータ23は、所定の圧縮方式（例えば、MP EG（Moving Picture Expert Group）方式）で圧縮され、さらにタイ

トルキー 2 2 を用いたスクランブルがかけられた状態のものである。そこで、まず、デスクランブル部 3 4 は、タイトルキー 2 2 を用いて、データ 2 3 にかけているスクランブルを解除する。

【 0 0 1 0 】

スクランブルが解除されたデータ 2 3 は、デコーダ 3 5 に供給される。デコーダ 3 5 は、所定のデコード方式（例えば、M P E G 方式）により、デスクランブル部 3 4 からのデータ 2 3 をデコードする。デコードされたデータ 3 6 は、図示されていないディスプレイなどに供給される。

【 0 0 1 1 】

図 1 に示したプレーヤ 1 2 は、例えば、DVD などのディスク 1 1 を専用に再生するような機器であるが、そのような専用のプレーヤ 1 2 に限らず、例えば、パーソナルコンピュータなどもディスク 1 1 を再生する機能を有している場合がある。

【 0 0 1 2 】

図 2 は、DVD などのディスク 1 1 をパーソナルコンピュータなどで再生する場合の構成例を示す図である。ここでは、ディスク 1 1 に記録されているデータを読み出す装置をドライブ装置 5 1 とし、ドライブ装置 5 1 により読み出されたデータを処理する装置をホスト (Host) 5 2 と記述する。図 2 に示したドライブ装置 5 1 やホスト 5 2 には、アプリケーションなどにより実現される機能も含まれている。

【 0 0 1 3 】

ディスク 1 1 には、図 1 に示した場合と同様に、ディスクキー 2 1、タイトルキー 2 2、および、データ 2 3 が記録されている。ドライブ装置 5 1 は、認証 (Authentication) 処理部 6 2、バス暗号化 (Bus Encrypt) 部 6 2、および、バス暗号化部 6 3 を有する構成とされている。

【 0 0 1 4 】

ホスト 5 2 は、認証処理部 7 1、バス復号 (Bus Decrypt) 部 7 2、バス復号部 7 3、復号 (Decrypt) 部 7 4、復号部 7 5、デスクランブル部 7 6、および、デコーダ 7 7 を有する構成とされている。また、ホスト 5 2 は、マスタキー 3 1 を管理する管理部 (不図示) も有している。

【 0 0 1 5 】

ドライブ装置 5 1 の認証処理部 5 1 とホスト 5 2 の認証処理部 7 1 は、相互認証処理を実行し、その認証処理が正常に行われたときだけ、データの授受を行う。認証処理が正常に行われると、セッションキーと称されるキーが、それぞれの認証処理部 6 1, 7 1 において発行 (共用) される。

【 0 0 1 6 】

認証処理が正常に行われた後の時点で、ディスク 1 1 から読み出されたディスクキー 2 1 は、ドライブ装置 5 1 のバス暗号化部 6 2 により暗号化される。バス暗号化部 6 2 には、認証処理部 6 1 において発行されたセッションキーも供給される。バス暗号化部 6 2 は、読み出されたディスクキー 2 1 を、セッションキーを用いて暗号化し、ホスト 7 1 に対して出力する。

【 0 0 1 7 】

同様に、バス暗号化部 6 3 は、ディスク 1 1 から読み出されたタイトルキー 2 2 を、認証処理部 6 1 が発行したセッションキーを用いて暗号化し、ホスト 5 2 に対して出力する。ディスク 1 1 から読み出されたデータ 2 3 は、直接的に、ドライブ装置 5 1 からホスト 5 2 に対して供給される。

【 0 0 1 8 】

ホスト 5 2 のバス復号部 7 2 は、ドライブ装置 5 1 のバス暗号化部 6 2 から供給された暗号化されているディスクキー 2 1 を、認証処理部 7 1 により発行されたセッションキーを用いて復号する。復号されたディスクキー 2 1 は、復号部 7 4 に供給される。復号部 7 4 には、マスタキー 3 1 も供給される。復号部 7 4 は、バス復号部 7 2 から供給されたディスクキー 2 1 を、マスタキー 3 1 を用いて復号し、その復号したディスクキー 2 1 を復

号部 75 に供給する。

【0019】

復号部 75 には、バス復号部 73 からのタイトルキー 22 も供給されるが、そのタイトルキー 22 は、バス復号部 73 が、認証処理部 71 により発行されたセッションキーを用いて復号したものである。

【0020】

復号部 75 は、復号されたディスクキー 21 により、暗号化されているタイトルキー 22 を復号する。復号されたタイトルキー 22 は、デスクランブル部 76 に供給される。デスクランブル部 76 には、ディスク 11 から読み出されたデータ 23 も供給される。

【0021】

ディスク 11 から読み出されるデータ 23 は、所定の圧縮方式で圧縮され、さらにタイトルキー 22 を用いたスクランブルがかけられた状態のものである。そこでまず、デスクランブル部 76 は、供給されたタイトルキー 22 を用いて、データ 23 にかけているスクランブルを解除する。

【0022】

スクランブルが解除されたデータ 23 は、デコーダ 77 に供給される。デコーダ 77 は、所定のデコード方式（例えば、MPEG 方式）により、供給されたデータ 23 をデコードする。デコードされたデータ 36 は、図示されていないディスプレイなどに供給される。

【0023】

このように、ディスク 11 がセットされるドライブ装置 51 と、ディスク 11 に記録されているデータを処理するホスト 52 により、ディスク 11 に記録されているデータ 23 の再生の処理が実行される場合、認証処理が行われ、その認証処理が正常に行われた後に、暗号化されたキーやデータの授受が行われる。

【0024】

認証処理が行われた後に、実際のデータの授受が行われるのは、ドライブ装置 51 とホスト 52 は、所定のバス（不図示）により接続されているが、そのバスを介して授受されるデータが盗用されないようにするためである。

【0025】

ここで、認証処理部 61 と認証処理部 71 との間で行われる認証処理について、図 3 のフローチャートを参照して説明を加える。ステップ S11 において、ディスク 11 が、ドライブ装置 51 に挿入（セット）されたか否かが判断される。ステップ S11 において、ディスク 11 が、ドライブ装置 51 に挿入されたと判断されるまで、待機状態が維持される（ステップ S11 における処理が繰り返される）。

【0026】

ステップ S11 において、ディスク 11 が、ドライブ装置 51 に挿入されたと判断された場合、ステップ S12 に処理が進められる。ステップ S12 において、認証処理部 61 と認証処理部 71 により、相互認証の処理が実行される。この相互認証の処理が正常に終了されなければ、これ以降の処理は実行されない。

【0027】

相互認証の処理が正常に終了されると、認証処理部 61 と認証処理部 71 のそれぞれにおいて、セッションキーが生成される。このような相互認証の処理とセッションキーの発生の処理が完了したか否かが、ステップ S13 において判断される。ステップ S13 において、ステップ S12 における処理は完了したと判断されるまで、ステップ S12 の処理が繰り返され、完了したと判断された場合、ステップ S14 に処理が進められる。

【0028】

ステップ S14 において、スクランブルされたデータの授受（ドライブ装置 51 からの出力）が許可された状態に設定される。この場合、スクランブルされたデータとは、データ 23（図 2）のことであり、このデータ 23 のドライブ装置 51 からホスト 52 への出力が許可された状態に設定される。

【0 0 2 9】

“許可された状態”ということについて説明を加える。データ 2 3 の読み出しは、ホスト 5 2 からの指示に基づいてドライブ装置 5 1 が行う。許可される前の状態において、ドライブ装置 5 1 は、仮にホスト 5 2 からデータ 2 3 の読み出し（出力）の指示を受けたとしても、エラーを返すだけで、データ 2 3 の出力は行わない。

【0 0 3 0】

許可された後の状態においては、ホスト 5 2 からデータ 2 3 の読み出した指示されれば、ドライブ装置 5 1 は、ディスク 1 1 からデータ 2 3 を読み出し、ホスト 5 2 に対して出力を行う。

【0 0 3 1】

このような状態に設定されると、ディスク 1 1 がドライブ装置 5 1 から排出されるなどの割り込み処理が発生しない限り、スクランブルされたデータ 2 3 の再生の処理が繰り返される。

【0 0 3 2】

スクランブルされたデータ 2 3 の出力が許可された状態にされると、ステップ S 1 5 において、ディスク 1 1 がドライブ装置 5 1 から排出された否かの判断が継続的に行われる。そして、ステップ S 1 5 において、ディスク 1 1 がドライブ装置 5 1 から排出されたと判断されると、ステップ S 1 1 に処理が戻され、それ以降の処理が繰り返される。

【0 0 3 3】

なお、ドライブがリセットされた場合や、電源がオフの状態にされた場合も、再生の処理が終了され、必要に応じ、ステップ S 1 1 に処理が戻され、それ以降の処理が繰り返される。

【0 0 3 4】

このようにして、ドライブ装置 5 1 とホスト 5 2 との間で認証処理が正常に終了されると、ドライブ装置 5 1 側では、ディスク 1 1 が排出されるまで、その挿入されているディスク 1 1 からデータ 2 3 を読み出し、その読み出したデータ 2 3 をホスト 5 2 に出力するという処理を、ホスト 5 2 からの指示がある限り継続的に行なわれる。

【0 0 3 5】

ここで、バス暗号化部 6 2 などの暗号化部において行われる公知の暗号化技術について説明を加える。暗号化の方式は、さまざまなものが提案されている。ここでは、C B C (Cipher Block Chaining) 方式を例に挙げて、暗号化（復号）の方式について説明する。

【0 0 3 6】

暗号化の一方式である C B C 方式は、ブロック連鎖のための一つの技法であり、排他的論理和演算により、平文の現在のブロックに暗号文の前のブロックを付加して、暗号文の各ブロックを作成する方式である。図 4 は、C B C 方式を用い暗号化を行う回路の一例を示す図である。

【0 0 3 7】

暗号化すべきデータは、所定の単位（例えば、ブロック暗号方式として A E S (Advanced Encryption Standard) を用いた場合は 1 6 バイト）毎にブロック化される。そして、第 1 のブロックは、排他的論理和回路 1 0 1 - 1 に供給され、第 1 のブロックに続く第 2 のブロックは、排他的論理和回路 1 0 1 - 2 に供給され、第 2 のブロックに続く第 3 のブロックは、排他的論理和回路 1 0 1 - 3 に供給されというように、所定の段数（ここでは、N 段とする）だけ設けられた排他的論理和回路 1 0 1 - 1 乃至 1 0 1 - N に順次、ブロック化された平文のデータが入力される。

【0 0 3 8】

排他的論理和回路 1 0 1 - 1 から出力された第 1 のブロックは、暗号化部 1 0 2 - 1 に供給される。暗号化部 1 0 2 - 1 は、鍵 E_k で供給された第 1 のブロックを暗号化する。このようにして、第 1 のブロックは暗号化される。

【0 0 3 9】

暗号化部 1 0 2 - 1 から出力された暗号化された第 1 のブロックは、排他的論理和回路

1 0 1 - 2 にも供給され、第 2 のブロックとの間で排他的論理和が演算される。その結果は、暗号化部 1 0 2 - 2 に供給され、同じく鍵 E_k で暗号化される。

【0 0 4 0】

このように、CBC方式における暗号化は、1つ前で暗号化したブロックと暗号化対象の現在の平文のブロックとの排他的論理和が演算されてから、そのブロックに対して所定の暗号化鍵での暗号化が行なわれるようになっている。結果の暗号文は次のブロックとの排他的論理和の演算に使われることになる。このように前のブロックと次々に連鎖させることにより暗号文が生成される。

【0 0 4 1】

第 2 のブロック以降は、前のブロックとの排他的論理和が演算されるが、第 1 のブロックは、前のブロックが存在しないため、前のブロックとの排他的論理和を演算することができない。そこで、第 1 のブロックに対しては、初期ベクトル (IV: Initializing Vector) を与えて排他的論理和を演算するように構成される。

【0 0 4 2】

次に、CBC方式を用い復号を行う回路（例えば、バス復号部 7 2 (図 2)）について、図 5 を参照して説明する。

【0 0 4 3】

上述したようにして暗号化されたデータは、所定の単位（例えば、ブロック暗号方式として AES (Advanced Encryption Standard) を用いた場合は 16 バイト）毎にブロック化されている。ブロック化されているデータの内、第 1 のブロックは、復号部 1 2 2 - 1 に供給され、第 1 のブロックに続く第 2 のブロックは、復号部 1 2 2 - 2 に供給され、第 2 のブロックに続く第 3 のブロックは、復号部 1 2 2 - 3 に供給されというように、所定の段数（ここでは、N 段とする）だけ設けられた復号部 1 2 2 - 1 乃至 1 2 2 - N に順次、暗号化されたブロック単位のデータが入力される。

【0 0 4 4】

各復号部 1 2 2 - 1 乃至 1 2 2 - N は、入力されたデータを鍵 D_k で復号する。各復号部 1 2 2 - 1 乃至 1 2 2 - N から出力されたデータは、対応する排他的論理和回路 1 2 1 - 1 乃至 1 2 1 - N に供給される。排他的論理和回路 1 2 1 - 2 乃至 1 2 1 - N には、前の段の復号部 1 2 2 - 1 乃至 1 2 2 - N-1 に供給されるデータも供給される。

【0 0 4 5】

このように、CBC方式の復号は、1つ前の暗号化されているブロックと復号対象の現在の復号されたブロックとの排他的論理和が演算されることにより、最終的な復号が行われる。

【0 0 4 6】

第 2 のブロック以降は、前のブロックとの排他的論理和が演算されるが、第 1 のブロックは、前のブロックが存在しないため、前のブロックとの排他的論理和を演算することができない。そこで、第 1 のブロックに対しては、初期ベクトル IV を与えて、排他的論理和が演算される構成とされている。

【0 0 4 7】

このようにして、暗号化、復号が行われている。

【特許文献 1】特許第 3 2 5 2 7 0 6 号明細書

【発明の開示】

【発明が解決しようとする課題】

【0 0 4 8】

ところで、図 2 に示したように、ドライブ装置 5 1 とホスト 5 2 によりディスク 1 1 に記録されているデータ 2 3 の再生の処理が実行される場合、図 3 のフローチャートを参照して説明したように、ドライブ装置 5 1 とホスト 5 2 における相互認証の処理が正常に終了されると、ドライブ装置 5 1 からのデータ 2 3 の出力が許可された状態にされる。

【0 0 4 9】

ここで、図 6 を参照して説明するに、ホスト 5 2 側でアプリケーション A が起動され、

そのアプリケーション A により、認証処理部 7 1 で行う認証処理が実行される場合を考える。アプリケーション A によるドライブ装置 5 1 との認証処理が正常に実行されると、ドライブ装置 5 1 からディスク 1 1 からデータ 2 3 が読み出され、出力されるといった処理が許可された状態にされる。

【0 0 5 0】

許可された状態のときに、ディスク 1 1 がドライブ装置 5 1 から排出されるなどの状況が発生しない限り、ドライブ装置 5 1 からデータ 2 3 が出力されるといった処理が許可された状態が維持される。そのような許可が維持されている状態のときに、アプリケーション B がホスト 5 2 側で起動されたとする。そして、アプリケーション A にかわり、アプリケーション B により、データ 2 3 の読み出しの指示などの処理が開始されたとする。

【0 0 5 1】

ドライブ装置 5 1 とアプリケーション B は、認証処理を行っていないにもかかわらず、ドライブ装置 5 1 は、データ 2 3 の出力が許可された状態に維持されているため、ドライブ装置 5 1 からホスト 5 2（アプリケーション B）に対して、データ 2 3 は出力されてしまう。その結果、例えば、ホスト 5 2 が有する HDD（Hard Disc Drive）1 4 1 にデータ 2 3 が記憶されるといった処理が、アプリケーション B により実行される可能性がある。

【0 0 5 2】

この HDD 1 4 1 に対するデータ 2 3 の記憶が不正な処理であっても、ドライブ装置 5 1 は、アプリケーション B の指示に基づき、データ 2 3 を出力してしまう。よって、このような不正を防ぐことができないといった課題があった。

【0 0 5 3】

また、HDD 1 4 1 に記憶されたデータ 2 3 は、スクランブルがかけられた状態であるため、そのままでは再生することができないが、スクランブルを解除するアプリケーションなども存在しているため、実質的には、HDD 1 4 1 にデータ 2 3 が記憶された時点で、不正に利用されてしまうことを防ぐことができないといった課題があった。

【0 0 5 4】

このように、一旦、正常に認証処理が行われ、ドライブ装置 5 1 側でデータ 2 3 の出力が許可された状態にされると、データ 2 3 が盗用されてしまう可能性があるといった課題があった。

【0 0 5 5】

図 7 を参照し、他のデータの盗用について説明する。ドライブ装置 5 1 とホスト 5 2 は、所定のバスにより接続され、そのバスを介してデータ 2 3 の授受を行うように構成されている。図 6 を参照して説明した場合と同様に、アプリケーション A により、ドライブ装置 5 1 との認証処理が行われる。そして、その認証処理が正常に行われると、ドライブ装置 5 1 からデータ 2 3 を出力するといった処理を実行することが許可された状態とされる。

【0 0 5 6】

バス上を授受されるデータをモニタする機能をホスト 5 2 が有していると、そのモニタ 1 5 1 により、バス上で授受されているデータ 2 3 をモニタする（取得する）ことが可能である。換言すれば、ドライブ装置 5 1 から出力されたデータ 2 3 は、アプリケーション A とモニタ 1 5 1 に供給されるといった状態にすることが可能である。

【0 0 5 7】

そのため、ホスト 5 2 側で、モニタ 1 5 1 により取得されたデータ 2 3 を、HDD 1 4 1 に記憶させるといった処理を実行することも可能となる。よって、このようにしてデータ 2 3 が盗用されてしまう可能性もある。

【0 0 5 8】

このように、バス上を授受されるデータが、モニタ機能により盗用されてしまう可能性があるといった課題があった。

【0 0 5 9】

バス上のデータが盗用されてしまうようなことを防ぐために、バスを介して授受されるデータ 23 を暗号化する方法も提案されている。図 8 を参照して説明する。ドライブ装置 51 側からホスト 52 に出力されるデータを転送データ 171 と記述する。

【0060】

転送データ 171 は、2048 バイト (2 K バイト) のデータパケット (data Packet) とされる。上述したように、ドライブ装置 51 とホスト 52 は、所定のバスで接続されているわけだが、そのバスをコントロールするバスインタフェース 183 は、所定の単位量のデータを取り扱うように規定されている。その単位量は、例えば、ATAPI (AT Attachment with Packet Interface) をバスインタフェース 183 として用いた場合、2048 バイトと規定されている。

【0061】

そこで、転送データ 171 を 2048 バイトで構成されるデータパケットとした場合、図 8 に示すように、1 パケットは、16 バイトの初期ベクトル IV と 2032 バイトのデータから構成される。このようなデータパケットのうち、2032 バイトのデータ部分が、暗号化部 181 により暗号化される。暗号化部 181 は、図 8 には図示していないが、認証処理部 181 (図 2) により発行されるセッションキー Ks を用いて暗号化を行う。

【0062】

暗号化部 181 は、例えば、CBC 方式を用いて暗号化を行う。CBC 方式に基づいて暗号化を行う場合、暗号化部 181 の内部構成例は、図 4 に示したようになる。図 4 を参照して説明したように、暗号化部 181 は、初期ベクトル IV も用いて暗号化を行う。すなわち、暗号化部 181 は、転送データ 171 のデータパケットの内、2038 バイトのデータ部分を、同じくデータパケット内に含まれる 16 バイトの初期ベクトル IV と、認証処理部 181 により発行されるセッションキー Ks を用いて暗号化を行う。

【0063】

暗号化部 181 により暗号化されたデータパケットも、2048 バイトのデータである。よって、その暗号化されたデータパケットは、バスインタフェース 183 により取り扱うことができる。データ部分が暗号化されたデータパケットは、ホスト 52 側の復号部 182 に供給される。復号部 182 は、供給されたデータパケットに含まれる初期ベクトル IV と、認証処理部 71 (図 2) により発行されるセッションキー Ks を用いて、暗号化されているデータの復号を行う。

【0064】

このようにして、ホスト 52 側は、暗号化されたデータを受信するが、そのデータと共に供給される初期ベクトル IV を用いて復号することができるため、ホスト 52 側において、ドライブ装置 51 側から出力されたデータを再生することができる。

【0065】

このように、バスインタフェース 183 上で授受されるデータを、暗号化されたデータとすることにより、仮に、バスインタフェース 183 を介して授受されるデータが盗聴されても、暗号化を解くことができなければ、盗用されることがなく、結果として、データが不正に利用されるような不都合が発生するようなことを防ぐことが可能となる。しかしながら、以下のような問題点がある。

【0066】

再度、図 8 を参照するに、初期ベクトル IV は、転送データ 171 に含まれている。転送データ 171 に初期ベクトル IV を含ませる場合、ディスク 11 に、他のデータと共に書き込まれている。よって、初期ベクトル IV をランダムに変化させることができない (書き込まれている初期ベクトル IV をそのまま用いなくてはならず、変化させることができない) といった問題があった。

【0067】

また、ディスク 11 に初期ベクトル IV が書き込まれているのではなく、ドライブ装置 51 側でランダムに初期ベクトル IV を発生させ、その初期ベクトル IV を転送データ 171 内に含ませるようにすることも考えられ。しかしながら、転送データ 171 に初期ベ

クトル I V を含ませる場合、暗号化されるデータと区別するために、例えば、ヘッダなどを付けなくてはならないなどの条件がある。

【0068】

そのような条件があるために、ドライブ装置 51 側で、ランダムに初期ベクトル I V を発生させるようにしても、ランダムに変化させることに対する制限があり、結果的には、ランダムに初期ベクトル I V を発生させるということに対してそのランダム性を保証することができない（固定パターンになってしまう）といった問題があった。

【0069】

初期ベクトル I V をランダムに変化させることができない場合、換言すれば、初期ベクトル I V として固定パターンが用いられるようにすると、以下のような問題が発生する可能性がある。

【0070】

例えば、電子メールを例に挙げて考える。電子メールの書式には、宛先、送信元、件名、本文といったような一連のパターンがある。そのようなパターンがあるようなデータ（平文）を暗号化した場合、暗号化されたデータ自体もパターンがあるデータとなってしまう。第 3 者（攻撃者）が、そのようなパターンに注目することにより、暗号文から平文の一部を解読することが可能である。

【0071】

また、音楽データなどで、その音楽データを繰り返し再生するような場合、結果として同じ平文を同じように暗号化することになり、暗号化されたデータ自体も同じ結果となる。そのため、上述した場合と同様に、暗号文から平文を解読することが可能である。

【0072】

そこで、パターンがあるような平文（同一のデータを複数回暗号化するような場合）でも、暗号化されたデータ（暗号文）にパターンがないようにするために、最初のブロックに初期ベクトル I V を加えるようにする。初期ベクトル I V を加えて暗号化を実行することにより、平文のブロックに同じパターンがあっても暗号文には同じパターンが発生しないので、暗号解読を困難にさせることが出来る。また、単一の鍵で大量のデータを暗号化した場合に暗号鍵が予測しやすくなる、という解読行為を、初期ベクトル I V を加えて暗号化を行うようにすることで防止することができるという効果もある。

【0073】

このような理由で最初のブロックに初期ベクトル I V が加えられ、その後の暗号化が行われるように構成されている場合が多い。

【0074】

そして、初期ベクトル I V を適当に更新させることで、平文のデータが特別なパターンのデータであることを特定させることを困難とし、データのすり替え、データの改竄行為を防止することができるとされている。（参考文献：NIST Special Publication 800-38A 2001 Edition, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, APPENDIX C Generation of Counter Blocks）

【0075】

よって、同じ初期ベクトル I V が繰り返し用いられると、結果として、初期ベクトル I V を適当に更新させることで、平文のデータが特別なパターンのデータであることを特定させることを困難とし、データのすり替え、データの改竄行為を防止することができないといった課題があった。

【0076】

また、上述したように、初期ベクトル I V は、更新される方が好ましいといった課題があった。

【0077】

そこで、初期ベクトル I V を更新できるようにした場合、図 9 に示すようなデータの授受の方法が考えられる。すなわち、図 9 に示した例では、転送データ 191 は、2048 バイトのデータから構成され、そのデータに、16 バイトの初期ベクトル I V が付加され

る。そして、初期ベクトル I V が付加された結果、2064 バイトにされたデータが、バスインタフェース 183 を介して授受される。

【0078】

初期ベクトル I V を転送データ 191 に付加する構成とすることにより（転送データ 191 に初期ベクトル I V を予め含めるような構成としないことにより）、初期ベクトル I V を、ドライブ装置 51 側でランダムに発生し、そのランダムに発生された初期ベクトル I V を付加させることができるようになる。

【0079】

しかしながら、このようにして初期ベクトル I V をデータに付加することは、例えば 2048 バイト単位の PC Drive Interface に、2064 バイト（I V = 16 バイトの場合）という特殊なセクタサイズを持ち込むことになり、標準的なフォーマットから外れてしまうこととなる。そのために、共通の ATAPI Device Driver を利用できない、UDF (Universal Data Format) で扱うことのできるセクタサイズである 2048 バイトや 4096 バイトに当てはまらないため UDF FS Driver を利用できないなど、パーソナルコンピュータにおける環境との相性がよくないといった課題があった。

【0080】

相性が良くないといったことを解決するためには、ハードウェア的に、ソフトウェア的にも特殊なものに変えなくてはならないなど、コスト的に割高になり、互換性を取りづらい、処理的に手間がかかるといった課題もあった。

【0081】

本発明はこのような状況に鑑みてなされたものであり、認証処理が正常に終了し、ドライブ装置側からデータが出力されることが許可された状態にされた後においても、その許可状態を解除できるようにし、データの盗用を防ぐことを目的とする。また、汎用なバスを用いた場合においても、初期ベクトル I V を更新できるようにし、そのバス上で授受されるデータが盗用されないようなセキュリティを高めることを目的とする。

【課題を解決するための手段】

【0082】

本発明の情報処理装置は、データの転送を制御する転送制御手段と、転送制御手段がデータの転送を制御した回数をカウントするカウント手段と、カウント手段によりカウントされた回数が、所定の閾値以上になったか否かを判断する第 1 の判断手段と、第 1 の判断手段により回数が閾値以上になったと判断された場合、転送制御手段に、データの転送を停止するように指示を出す第 1 の指示手段と、転送制御手段により転送が制御されるデータの暗号化または復号に用いられる初期ベクトルを生成する生成手段と、転送制御手段により転送が制御されるデータを授受する他の装置から、初期ベクトルの供給が指示されたか否かを判断する第 2 の判断手段と、第 2 の判断手段により初期ベクトルの供給が指示されたと判断された場合、生成手段に初期ベクトルの生成を指示するとともに、カウント手段によりカウントされている回数をリセットするように指示を出す第 2 の指示手段とを備えることを特徴とする。

【0083】

前記第 1 の指示手段による指示が出された場合、他の装置に対してデータの転送が停止されたことを示すメッセージを出力する出力手段をさらに備えるようにすることができる。

【0084】

本発明の情報処理方法は、データの転送を制御する転送制御ステップと、転送制御ステップの処理でデータの転送が制御された回数をカウントするカウントステップと、カウントステップの処理によりカウントされた回数が、所定の閾値以上になったか否かを判断する第 1 の判断ステップと、第 1 の判断ステップの処理で回数が閾値以上になったと判断された場合、転送制御ステップにおける処理で、データの転送が停止されるように指示を出す第 1 の指示ステップと、転送制御ステップの処理で転送が制御されるデータの暗号化または復号に用いられる初期ベクトルを生成する生成ステップと、転送制御ステップの処理

で転送が制御されるデータを授受する他の装置から、初期ベクトルの供給が指示されたか否かを判断する第2の判断ステップと、第2の判断ステップの処理で初期ベクトルの供給が指示されたと判断された場合、生成ステップによる処理で初期ベクトルが生成されるように指示するとともに、カウンタステップの処理によりカウントされている回数がリセットされるように指示を出す第2の指示ステップとを含むことを特徴とする。

【0085】

本発明のプログラムは、データの転送を制御する転送制御ステップと、転送制御ステップの処理でデータの転送が制御された回数をカウントするカウントステップと、カウントステップの処理によりカウントされた回数が、所定の閾値以上になったか否かを判断する第1の判断ステップと、第1の判断ステップの処理で回数が閾値以上になったと判断された場合、転送制御ステップにおける処理で、データの転送が停止されるように指示を出す第1の指示ステップと、転送制御ステップの処理で転送が制御されるデータの暗号化または復号に用いられる初期ベクトルを生成する生成ステップと、転送制御ステップの処理で転送が制御されるデータを授受する他の装置から、初期ベクトルの供給が指示されたか否かを判断する第2の判断ステップと、第2の判断ステップの処理で初期ベクトルの供給が指示されたと判断された場合、生成ステップによる処理で初期ベクトルが生成されるように指示するとともに、カウンタステップの処理によりカウントされている回数がリセットされるように指示を出す第2の指示ステップとを含む処理をコンピュータに実行させることを特徴とする。

【0086】

本発明の記録媒体のプログラムは、データの転送を制御する転送制御ステップと、転送制御ステップの処理でデータの転送が制御された回数をカウントするカウントステップと、カウントステップの処理によりカウントされた回数が、所定の閾値以上になったか否かを判断する第1の判断ステップと、第1の判断ステップの処理で回数が閾値以上になったと判断された場合、転送制御ステップにおける処理で、データの転送が停止されるように指示を出す第1の指示ステップと、転送制御ステップの処理で転送が制御されるデータの暗号化または復号に用いられる初期ベクトルを生成する生成ステップと、転送制御ステップの処理で転送が制御されるデータを授受する他の装置から、初期ベクトルの供給が指示されたか否かを判断する第2の判断ステップと、第2の判断ステップの処理で初期ベクトルの供給が指示されたと判断された場合、生成ステップによる処理で初期ベクトルが生成されるように指示するとともに、カウンタステップの処理によりカウントされている回数がリセットされるように指示を出す第2の指示ステップとを含むことを特徴とする。

【0087】

本発明の情報処理装置および方法、並びにプログラムにおいては、初期ベクトルの供給の指示が定期的に行われなければ、データの授受が停止される。

【発明の効果】**【0088】**

本発明によれば、装置間での転送路上におけるセキュリティを高めることが可能となる。

【0089】

また、本発明によれば、記録媒体を扱う装置とその装置からのデータを扱う他の装置との間で認証処理が行われた後、記録媒体を扱う装置側で、記録媒体から読み出したデータを他の装置に出力することが許可された状態にされても、その状態を解除（更新）することが可能となる。もって、一旦、他の装置へのデータの出力が許可された状態であっても、その後の不正なアクセスによるデータの流出を防ぐことが可能となる。

【0090】

また、本発明によれば、暗号化の際に用いられる初期ベクトルをランダムに更新することができ、同一のデータを暗号化しても、同一の暗号文が生成されるようなことを防ぐことが可能となる。もってデータのすり替え、データの改竄行為などの不正な処理を防止することができる。

【0091】

また、本発明によれば、初期ベクトルを更新するようにしても、汎用のバスインタフェースおよびOS(Operating System)で標準的に用意されたUDF FS Driverを利用できる。もって、初期ベクトルを更新できるようにするために、装置間の環境を変更しなくてはならないといったような不都合が発生するようなことを防ぐことができる。

【発明を実施するための最良の形態】

【0092】

以下に本発明の最良の形態を説明するが、開示される発明と実施の形態との対応関係を例示すると、次のようになる。明細書中には記載されているが、発明に対応するものとして、ここには記載されていない実施の形態があったとしても、そのことは、その実施の形態が、その発明に対応するものではないことを意味するものではない。逆に、実施の形態が発明に対応するものとしてここに記載されていたとしても、そのことは、その実施の形態が、その発明以外の発明には対応しないものであることを意味するものでもない。

【0093】

さらに、この記載は、明細書に記載されている発明の全てを意味するものではない。換言すれば、この記載は、明細書に記載されている発明であって、この出願では請求されていない発明の存在、すなわち、将来、分割出願されたり、補正により出現し、追加される発明の存在を否定するものではない。

【0094】

本発明を適用した情報処理装置は、データの転送を制御する転送制御手段（例えば、図13のステップS46の処理を実行する図10のセクタ転送制御部313）と、転送制御手段がデータの転送を制御した回数をカウントするカウント手段（例えば、図13のステップS47の処理を実行する図10のセクタ転送カウンタ314）と、カウント手段によりカウントされた回数が、所定の閾値以上になったか否かを判断する第1の判断手段（例えば、図13のステップS45の処理を実行する図10のセクタ転送カウンタ314）と、第1の判断手段により回数が閾値以上になったと判断された場合、転送制御手段に、データの転送を停止するように指示を出す第1の指示手段（例えば、図10のセクタ転送カウンタ314）と、転送制御手段により転送が制御されるデータの暗号化または復号に用いられる初期ベクトルを生成する生成手段（例えば、図13のステップS41の処理を実行する図10の乱数発生部315）と、転送制御手段により転送が制御されるデータを授受する他の装置から、初期ベクトルの供給が指示されたか否かを判断する第2の判断手段（例えば、図13のステップS40の処理を実行する図10のコマンド処理部317）と、第2の判断手段により初期ベクトルの供給が指示されたと判断された場合、生成手段に初期ベクトルの生成を指示するとともに、カウンタ手段によりカウントされている回数をリセットするように指示を出す第2の指示手段（例えば、図13のステップS42の処理を実行する図10の乱数発生315）とを少なくとも備える。

【0095】

前記第1の指示手段による指示が出された場合、他の装置に対してデータの転送が停止されたことを示すメッセージを出力する出力手段（例えば、図13のステップS48の処理を実行する図10のメッセージ伝達部316）をさらに備える。

【0096】

以下に、本発明の実施の形態について図面を参照して説明する。

【実施例1】

【0097】

図10は、本発明を適用したシステムの一実施の形態の構成を示す図である。

【0098】

図10に示したシステムは、所定の記録媒体に記録されたデータを再生する（読み出す）システムの構成例を示している。図10に示したシステムは、データを供給するドライブ装置301と、データの供給を受けるホスト302から構成されている。

【0099】

ディスク 303 は、例えば、CD-ROM (Compact Disc-ROM)、CD-R (Compact Disc-Recordable)、CD-RW (Compact Disc-ReWritable)、DVD-ROM (Digital Versatile Disc-ROM)、DVD-R (Digital Versatile Disc-Recordable)、DVD-RW (Digital Versatile Disc-Rerecordable)、DVD+R (DVD+Recordable)、DVD+RW (DVD+ReWritable)、DVD-RAM (Digital Versatile Disk-Random Access Memory)、Blu-Ray Disc などである。また、本発明の適用範囲はこれらの記録媒体に限定されるものではなく、他の形態 (記録方式、形状など) の記録媒体を扱うシステムにも適用可能である。

【0100】

ドライブ装置 301 とホスト 302 は、所定のインタフェースによりデータの授受が行えるように接続されている。所定のインタフェースとしては、例えば、ATAPI (AT Attachment with Packet Interface) を用いることができる。ATAPI は、IDE (Integrated Drive Electronics) や、ATA (AT Attachment) インタフェースに CD-ROM ドライブなどハードディスク以外の周辺機器を接続するためのデータ転送方式に従ったインタフェースであり、例えば SCSI から流用したコマンドをパケット化して IDE インタフェースに渡すことで周辺機器の制御を可能とする。同様のコマンドパケットは USB (Universal Serial Bus) や IEEE1394 などの物理インタフェースへも適用可能である。

【0101】

ドライブ装置 301 は、認証処理部 311、暗号化部 312、セクタ転送制御部 313、セクタ転送カウンタ 314、乱数発生部 315、メッセージ伝達部 316、コマンド処理部 317、および、アクセス処理部 318 を含む構成とされている。

【0102】

ホスト 302 は、認証処理部 321、復号部 322 を含む構成とされている。

【0103】

ドライブ装置 301 の認証処理部 311 とホスト 302 の認証処理部 321 により、相互認証に関わる処理が実行される。

【0104】

暗号化部 312 には、アクセス処理部 318 による処理により、ディスク 303 から読み出されたセクタデータ 351 と、認証処理部 311 からセッションキー Ks が供給される。また、暗号化部 312 には、乱数発生部 315 により発生された乱数が、初期ベクトル IV として供給される。

【0105】

なお、乱数発生部 315 により発生された乱数を、そのまま初期ベクトル IV として用いても良いが、乱数と他のデータ (例えば、ディスク 303 から読み出される PSN (Physical Sector Number) など) が用いられて生成されるものを初期ベクトル IV として用いられるようにしても良く、そのような処理を実行する部分を、ドライブ装置 301 内に設けるようにしても良い。

【0106】

暗号化部 313 は、供給されたセクタデータ 351 をセッションキー Ks と初期ベクトル IV を用いて暗号化し、セクタ転送制御部 313 に供給する。セクタ転送制御部 313 は、暗号化されたセクタデータ 351 を、ホスト 303 の復号部 322 に対して供給する。よって、ドライブ装置 301 からホスト 303 に供給されるデータは、暗号化されたセクタデータ 351 である。

【0107】

暗号化部 312 からは、セクタ転送カウンタ 314 にもデータが出力される。セクタ転送カウンタ 314 は、ホスト 302 に対して出力されたセクタデータ (暗号化部 312 から出力されたセクタデータ 351) の数をカウントするように構成されている。換言すれば、セクタ転送カウンタ 314 は、セクタ転送制御部 313 がセクタデータの転送を制御した回数をカウントする。

【0108】

また、セクタ転送カウンタ 314 は、予め設定されたカウント数の最大値 (N_{\max} とする) を管理しており、カウントしているセクタ数 (カウンタ値 N) が、その最大値を超えないか否かを常に監視している。

【0109】

セクタ転送カウンタ 314 は、 $N \geq N_{\max}$ になった場合、セクタ転送制御部 313 に対して、ホスト 302 へのセクタデータ 351 の出力を停止するように指示を出す。このような指示を出すとともに、セクタ転送カウンタ 314 は、コマンド処理部 317 に対して、アクセス処理部 318 によるディスク 303 へのアクセスを停止するように指示を出す。

【0110】

セクタ転送制御部 313 は、セクタ転送カウンタ 314 からセクタデータ 351 の出力の停止の指示を受けた場合、メッセージ伝達部 316 に対して、メッセージ 362 (この場合、エラーメッセージ) をホスト 302 に対して出力するように指示を出す。

【0111】

一方、ホスト 303 の復号部 322 は、ドライブ装置 301 からインタフェースを介して暗号化されたセクタデータ 351 の供給を受ける。復号部 322 は、ドライブ装置 301 から、セクタデータ 351 とは別の経路 (詳細は図 11 を参照して後述する) で、乱数発生部 315 により発生された初期ベクトル IV も供給される。

【0112】

復号部 322 は、認証処理部 331 から供給されるセッションキー K_s と、ドライブ装置 301 から供給された初期ベクトル IV を用いて復号処理を実行し、セクタデータ 361 を生成する。

【0113】

ホスト 302 からは、コマンドパケット 363 が必要に応じて、ドライブ装置 301 に対して供給される。このコマンドパケット 363 は、例えば、ディスク 303 からデータの読み出しを指示するリードコマンド (Read command)、ディスク 303 へのデータの書き込みを指示するライトコマンド (Write command)、初期ベクトル IV の発行を指示するレポートキーコマンド (Report Key command) などがある。

【0114】

図 11 を参照して、セクタデータ 351 が授受される経路と、その他のデータが授受される経路について説明する。PC driver 391 は、例えば、初期ベクトル IV の生成、暗号化セクタデータの作成、転送セクタデータの作成などを制御するドライバーである。PC driver 391 からのデータは、Optical Disc driver 392 に渡される。

【0115】

Optical Disc driver 392 は、光ディスク (Optical Disc) の読み出しや書き込みを制御するドライバーである。光ディスクが DVD などの記録媒体である場合、その光ディスクに書き込まれているデータ (ファイル) は、UDF (Universal Data Format) に準拠したものとされている。よって、Optical Disc driver 392 により読み出された (制御された) データ (ファイル) は、UDF FS driver 393 の制御により、Optical Disc file reader 394 を介して、Video/Audio Playback function 395 に渡される。

【0116】

Video/Audio Playback function 395 は、例えば、転送セクタデータの取得、初期ベクトル IV の取得、暗号化セクタデータの復号を制御する。

【0117】

このように、セクタデータなどの映像や音声に関わるデータは、UDF FS driver 393 を介して授受されるが、その他の、例えば、初期ベクトル IV やその初期ベクトル IV を発行させるためのコマンドなどのデータは、UDF FS driver 393 を介さずに授受される。この UDF FS driver 393 を介さずに行われるデータの授受の経路は、Microsoft Windows (登録商標) においては SCSI PASS Through などと称されている。

【0118】

図 1 0 において、ドライブ装置 3 0 1 とホスト 3 0 2 との間に図示されている線のうち、太線で示した経路が、UDF FS driver 3 9 3 を介してデータの授受が行われる経路（以下、適宜、UDF 経路と称する）を示し、細線で示した経路が、その他のデータの授受が行われる経路（SCSI PASS Through、以下、適宜、パス経路と称する）を示すとする。

【0 1 1 9】

図 1 0 に示したように、セクタ転送制御部 3 1 3 から復号部 3 2 2 への経路が UDF 経路である。認証処理部 3 1 1 と認証処理部 3 2 1 との間で行われる認証処理に必要とされるデータの授受は、パス経路を介して行われる。また、メッセージ伝達部 3 1 6 から出力されるメッセージ 3 6 2 は、パス経路を介して授受される。また、初期ベクトル I V も、パス経路を介して授受される。

【0 1 2 0】

UDF FS driver 3 9 3 は、2 0 4 8 バイトのデータ、または、2 0 4 8 バイトの整数倍のデータ容量のデータを取り扱う。よって、UDF 経路を介して授受されるデータは、2 0 4 8 バイトまたはその倍数のデータしか通すことができない。

【0 1 2 1】

これに対し、パス経路は、基本的にデータの容量にかかわらず授受することが可能である。よって、1 6 バイトで構成される初期ベクトル I V などを授受するのに適した経路である。

【0 1 2 2】

図 1 0 に示した構成のドライブ装置 3 0 1 の動作について、図 1 2 と図 1 3 のフローチャートを参照して説明する。ステップ S 3 1 において、ドライブ装置 3 0 1 にディスク 3 0 3 が、挿入されたか否かが判断される。ステップ S 3 1 において、ドライブ装置 3 0 1 にディスク 3 0 3 が挿入されたと判断された場合、ステップ S 3 2 に処理が進められ、ホスト 3 0 2 において所定のアプリケーションが起動されたか否かが判断される。

【0 1 2 3】

所定のアプリケーションとは、ドライブ装置 3 0 1 に挿入されたディスク 3 0 3 からデータを読み出す、または、書き込むために必要とされるアプリケーションである。

【0 1 2 4】

ステップ S 3 2 において、ホスト 3 0 2 において所定のアプリケーションが起動されたと判断された場合、ステップ S 3 3 に処理が進められる。ステップ S 3 3 において、ドライブ装置 3 0 1 とホスト 3 0 2 との間で相互認証処理が実行され、セッションキー K s が、ドライブ装置 3 0 1 とホスト 3 0 2 で、それぞれ生成（共用）される。ステップ S 3 4 において、セッションキー K s の生成が完了したか否かが判断される。セッションキー K s の生成が完了されるまで、ステップ S 3 3 とステップ S 3 4 の処理が繰り返される。

【0 1 2 5】

そして、ステップ S 3 4 において、セッションキー K s の生成が完了したと判断されると、ステップ S 3 5 に処理が進められ、ドライブ装置 3 0 1 のセクタ転送カウンタ 3 1 4 のカウンタ値 N が、予め設定されているカウンタ値 N の最大値である値 Nmax に設定される（N = Nmax に設定される）。

【0 1 2 6】

このように、N = Nmax に設定されると、セクタ転送カウンタ 3 1 4 の指示により、セクタ転送制御部 3 1 3 からホスト 3 0 2 へのデータの出力が許可されない状態に設定される。

【0 1 2 7】

ステップ S 3 6 において、ホスト 3 0 2 から初期ベクトル I V の転送要求があったか否かが判断される。この判断は、コマンド処理部 3 1 7 が、ホスト 3 0 2 側から、コマンドパケット 3 6 3 を受信したか否かを判断し、かつ、受信したコマンドパケット 3 6 3 が、初期ベクトル I V の転送要求を示すものであるか否かを判断することにより行われる。

【0 1 2 8】

ステップ S 3 6 において、初期ベクトル I V の転送要求があったと判断されるまで、ス

テップ S 3 6 の処理が繰り返される。そして、ステップ S 3 6 において、初期ベクトル I V の転送要求があったと判断された場合、ステップ 3 7 に処理が進められ、初期ベクトル I V の生成が行われる。

【0 1 2 9】

コマンド処理部 3 1 7 は、ホスト 3 0 2 からのコマンドパケット 3 6 3 を受信し、そのコマンドパケット 3 6 3 を解析することにより、初期ベクトル I V の転送要求であると判断すると、そのことを、乱数発生部 3 1 5 に知らせる。そのような知らせを受けた乱数発生部 3 1 5 は、ステップ S 3 7 の処理として、初期ベクトル I V を生成する。

【0 1 3 0】

乱数発生部 3 1 5 は乱数を発生するが、その乱数が、そのまま初期ベクトル I V とされる。または、発生された乱数と所定の情報（例えば、初期ベクトル I V の転送要求を指示するコマンドパケット 3 6 3 に含まれる情報）などを用い、排他的論理和を算出するなどの処理が実行されることにより、初期ベクトル I V が発生されるようにしても良い。

【0 1 3 1】

乱数発生部 3 1 5 は、初期ベクトル I V を生成すると共に、セクタ転送カウンタ 3 1 4 に対して、カウンタ数 N を 0 に設定し直すように指示を出す。このような指示を受け取ったセクタ転送カウンタ 3 1 4 は、ステップ S 3 8 の処理として、カウンタ値 N を 0 に設定し直す。このようにセクタ転送カウンタ 3 1 4 のカウンタ値 N が、0 に設定されると、セクタ転送制御部 3 1 3 からのデータの出力が許可された状態に変更される。

【0 1 3 2】

乱数発生部 3 1 5 により生成された初期ベクトル I V は、ステップ S 3 9 において、ホスト 3 0 2 に供給される。この初期ベクトル I V の供給（転送）は、パス経路を介して行われるため、例えば、初期ベクトル I V が 1 6 バイトで構成される場合であっても、その 1 6 バイトの初期ベクトル I V をドライブ装置 3 0 1 とホスト 3 0 2 側で授受することが可能である。

【0 1 3 3】

ステップ S 3 3 乃至 S 3 9 の処理のうち、初期ベクトル I V の授受に関わる処理について、図 1 4 を参照して説明を加える。

【0 1 3 4】

ホスト 3 0 2 は、ステップ S 1 0 1 において、ドライブ装置 3 0 1 は、ステップ S 1 1 1 において、それぞれ相互認証（Authentication）を行う。この相互認証が正常に行われた場合のみ、次のステップに処理が進められる。また、この相互認証の結果、ドライブ装置 3 0 1 の認証処理部 3 1 1 とホスト 3 0 2 の認証処理部 3 2 1 との、それぞれにおいてセッションキー K s が生成される（共有される）ことになる。

【0 1 3 5】

ホスト 3 0 2 は、ステップ S 1 0 2 において、コマンドパケット 3 6 3 を生成し、ドライブ装置 3 0 1 に対して出力する。ステップ S 1 0 2 において生成され、出力されるコマンドパケット 3 6 3 は、REPORT KEY command であり、この REPORT KEY command は、ここでは、初期ベクトル I V の転送を要求するものであるとする。

【0 1 3 6】

そのような REPORT KEY command を、ステップ S 1 1 2 の処理として受信したドライブ装置 3 0 1 は、ステップ S 1 1 3 において、初期ベクトル I V を生成する。生成された初期ベクトル I V は、ステップ S 1 1 4 において、ドライブ装置 3 0 1 からホスト 3 0 2 に対して出力される。この出力される初期ベクトル I V は、そのままホスト 3 0 2 側に出力される。

【0 1 3 7】

このようにしてドライブ装置 3 0 1 から出力された初期ベクトル I V を、ホスト 3 0 3 は、ステップ S 1 0 3 において受信する。

【0 1 3 8】

このように、ドライブ装置 3 0 1 からホスト 3 0 2 に転送される初期ベクトル I V を、

暗号化などの処理を施さずに、そのまま転送されるようにしても良いが、暗号化が施された状態で転送されるようにしてももちろん良い。

【0139】

初期ベクトル I V は、乱数発生部 315 により乱数を用いて発生されるため、ランダムに変化される値である。また、初期ベクトル I V は、セッションキー Ks と異なり、秘匿する必要性は低いと考えられる。このようなことを考慮し、図 14 を参照して説明したように、転送される初期ベクトル I V は、そのまま転送されるようにしても良い。

【0140】

しかしながら、初期ベクトル I V は、予測不可能であることが好ましいという条件がある。その条件を満たすために、転送される初期ベクトル I V を暗号化し、より安全性を高めるようにしてももちろん良い。

【0141】

より安全性を高めて初期ベクトル I V が転送されるようにした場合、図 15 に示すように処理が行われる。ホスト 302 側で行われるステップ S131 乃至 S133 における処理は、基本的に、図 14 におけるステップ S101 乃至 S103 と同様に行われるが、ステップ S103 において受信される初期ベクトル I V は、暗号化されているため、受信された後に、復号という処理が実行される点異なる。

【0142】

ドライブ装置 301 側で行われるステップ S141 乃至 S144 における処理も、基本的に、図 14 におけるステップ S111 乃至 S114 と同様であるが、ステップ S143 において、初期ベクトル I V が生成されたあと、その初期ベクトル I V が、セッションキー Ks が用いられて暗号化され、その暗号化された初期ベクトル I V ($E[Ks, IV]$) が、ステップ S144 における処理としてホスト 302 側に転送される点異なる。

【0143】

このようにして、ホスト 302 側から初期ベクトル I V の転送要求があると、ドライブ装置 301 は、初期ベクトル I V を生成し、ホスト 302 側に転送する。もちろん、ドライブ装置 301 は、生成した初期ベクトル I V を、ホスト 302 側に転送するだけでなく、自己の暗号化部 312 (図 10) にも供給する。

【0144】

図 12 のフローチャートの処理の説明に戻り、ステップ S39 における初期ベクトル I V の転送の処理が終了されると、ステップ S40 (図 13) に処理が進められる。ステップ S40 において、初期ベクトル I V の再発行要求があったか否かが判断される。ステップ S40 において、初期ベクトル I V の再発行要求があったと判断された場合、ステップ S41 乃至 S43 の処理が実行される。

【0145】

ステップ S41 乃至 S43 は、基本的に、ステップ S37 乃至ステップ S38 の処理と同様であるが、図 16 を参照して説明を加える。ホスト 301 は、ステップ S161 において、初期ベクトル I V の再発行要求をドライブ装置 301 に対して出す。この再発行要求は、コマンドパケット 363 が出力されることにより行われるが、このコマンドパケット 363 は、例えば、図 14 のステップ S102 において発行される REPORT KEY command と同じである。

【0146】

ドライブ装置 301 は、ステップ S171 において、REPORT KEY command を受信すると、ステップ S172 において、初期ベクトル I V を再生成する。初期ベクトル I V の再生成は、図 14 のステップ S113、または、図 15 のステップ S143 の処理と同様に行われる。そして、再生成された初期ベクトル I V は、ステップ S173 において、ホスト 302 側に転送される。この転送時に、初期ベクトル I V は、暗号化が施されて転送されるようにしても良いし、そのまま転送されるようにしても良い。

【0147】

図 13 のフローチャートの説明に戻り、ステップ S40 において、初期ベクトル I V の

再発行要求はないと判断された場合、または、ステップ S 4 3 における処理として初期ベクトル I V の転送に関わる処理が終了した場合、ステップ S 4 4 に処理が進められる。

【0 1 4 8】

ステップ S 4 4 において、セクタデータ 3 5 1 の転送要求があったか否かが判断される。この判断は、コマンド処理部 3 1 7 が、ホスト 3 0 2 側から、コマンドパケット 3 6 3 を受信したか否かを判断し、かつ、受信したコマンドパケット 3 6 3 が、セクタデータ 3 5 1 の転送を要求するものであるか否かを判断することにより行われる。

【0 1 4 9】

ステップ S 4 4 において、セクタデータ 3 5 1 の転送要求はないと判断された場合、ステップ 4 0 に処理が戻され、それ以降の処理が繰り返される。一方、ステップ S 4 4 において、セクタデータ 3 5 1 の転送要求があったと判断された場合、ステップ 4 5 に処理が進められる。

【0 1 5 0】

ステップ S 4 5 において、セクタ転送カウンタ 3 1 4 のカウンタ値 N が、 $N > N_{\max}$ という関係を満たすか否かが判断される。ステップ S 4 5 において、 $N > N_{\max}$ という関係は満たされていないと判断された場合、ステップ S 4 6 に処理が進められる。 $N > N_{\max}$ という関係が満たされていない状態、すなわち、 $N < N_{\max}$ という関係を満たす状態のときには、セクタ転送制御部 3 1 3 からのデータの出力（ホスト 3 0 2 側へのデータの転送）が許可されている状態である。

【0 1 5 1】

そこで、ステップ S 4 6 においては、セクタ転送制御部 3 1 3 からホスト 3 0 2 側へのデータの転送が行われる。まず、コマンド処理部 3 1 7 の指示により、アクセス処理部 3 1 8 が、ディスク 3 0 3 からセクタデータ 3 5 1 の読み出しの制御を行う。アクセス処理部 3 1 8 の制御により、ディスク 3 0 3 から読み出されたセクタデータ 3 5 1 は、暗号化部 3 1 2 に供給される。

【0 1 5 2】

暗号化部 3 1 2 は、認証処理部 3 1 1 から供給されるセッションキー Ks と、乱数発生部 3 1 5 から供給される初期ベクトル I V を用いて、セクタデータ 3 5 1 を暗号化する。暗号化されたセクタデータ 3 5 1 は、セクタ転送制御部 3 1 3 の制御により、ホスト 3 0 2 に転送される。この際、セクタデータ 3 5 1 が転送される経路は、UDF 経路であり、そのデータ量は、2 0 4 8 バイト（または、2 0 4 8 の整数倍のバイト数）とされている。

【0 1 5 3】

暗号化部 3 1 2 からデータが出力されると、その情報は、セクタ転送カウンタ 3 1 4 に供給される。セクタ転送カウンタ 3 1 4 は、ステップ S 4 7 において、自己が管理しているカウンタ値 N を、 $N + 1$ の値に更新し、その更新された値を新たなカウンタ値 N と設定する。セクタ転送カウンタ 3 1 4 におけるカウンタ値 N の更新が終了されると、ステップ S 4 0 に処理が戻され、それ以降の処理が繰り返される。

【0 1 5 4】

このセクタデータ 3 5 1 の転送に関わる処理について、図 1 7 のタイミングチャートを参照して、説明を加える。ホスト 3 0 2 は、ステップ S 2 0 1 において、リードコマンド (READ command) を発行する。リードコマンドは、ディスク 3 0 3 からセクタデータ 3 5 1 を指示する際に発行されるコマンドである。また、後述するように、ディスク 3 0 3 にデータを書き込む際にはライトコマンド (WRITE command) が発行される。

【0 1 5 5】

発行されるリードコマンドは、例えば、図 1 8 に示したデータ構成を有するコマンドパケット 3 6 3 の一種である。コマンドの詳細は INCITS T10 WORKING DRAFT “MultiMedia Command Set-4 (MMC-4)” に記述がある。

【0 1 5 6】

図 1 8 に示したコマンドパケット 3 6 3 は、リードコマンドまたはライトコマンドの形式を示すものである。図 1 8 に示したコマンドパケット 3 6 3 内のデータのうち、以下の

説明に必要な部分のデータについて説明を加える。

【0 1 5 7】

“Operation Code” には、リードコマンドであるか、ライトコマンドであるかを示すデータが書き込まれる。よって、この部分に書き込まれているデータを参照することで、ホスト 3 0 2 からコマンドを受け取ったドライブ装置 3 0 1 は、リードコマンドであるか、ライトコマンドであるかを判別することが可能となっている。また、“Operation Code” は、1 バイトのデータである

【0 1 5 8】

“Logical Block Address” には、コマンドパケット 3 6 3 がリードコマンドである場合には、読み出すべきアドレスの開始 L B A が書き込まれ、コマンドパケット 3 6 3 がライトコマンドである場合には、書き込むべきアドレスの開始 L B A が書き込まれている。また、“Logical Block Address” は、4 バイトのデータである。

【0 1 5 9】

“Transfer Length” には、コマンドパケット 3 6 3 がリードコマンドである場合には、読み出しセクタ数を指示するデータが書き込まれ、コマンドパケット 3 6 3 がライトコマンドである場合には、書き込みセクタ数を指示するデータが書き込まれる。また、“Transfer Length” は、4 バイトのデータである。

【0 1 6 0】

ステップ S 2 0 1 において、ホスト 3 0 2 から発行されるコマンドパケット 3 6 3 は、“Operation Code” がリードコマンドを示す値が記載されているコマンドである。ここでは、その発行されるリードコマンドに含まれる “Transfer Length” は “N 1” であるコマンドが発行されたとする。

【0 1 6 1】

ステップ S 2 0 1 における処理で発行されたリードコマンドは、ステップ S 2 3 1 において、ドライブ装置 3 0 1 のコマンド処理部 3 1 7 に供給される。コマンド処理部 3 1 7 は、供給されたコマンドの “Operation Code” を参照し、リードコマンドであることを認識する。そして、“Logical Block Address” を参照し、データの読み出しを開始するアドレスを認識し、“Transfer Length” を参照して、この場合、“Transfer Length” = N 3 ということ認識する。

【0 1 6 2】

コマンド処理部 3 1 7 は、認識結果を、アクセス処理部 3 1 8 に供給する。アクセス処理部 3 1 8 は、コマンド処理部 3 1 7 からの認識結果に基づき、ディスク 3 0 3 からのデータの読み出しを制御する。アクセス処理部 3 1 8 における処理としては、アドレスの変換処理などがある。

【0 1 6 3】

アクセス処理部 3 1 8 は、LBA/PSN変換を行う。L B A は、Logical Block Addressの略であり、P S N は、Physical Sector Numberの略である。L B A は、論理的なアドレスを示し、例えば、リードコマンドに含まれ、ディスク 3 0 3 上の読み出すべきデータの物理媒体に依存せずにドライブ装置 3 0 1 とホスト 3 0 2 との間で共通的に扱うことを可能とする論理的なアドレスを示す。

【0 1 6 4】

L B A に対し、P S N は、物理的なアドレスを示す。コマンドパケット 3 6 3 には、L B A が含まれるが、この L B A は、ディスク 3 0 3 上の論理的なアドレスを示し、実際の物理的なアドレスは示していないため、物理媒体から読み出した物理的なアドレスを示す P S N から共通に扱える論理的なアドレスへ変換するといった処理が、必要に応じ行われる。その変換処理を、アクセス処理部 3 1 8 は行う。

【0 1 6 5】

なお、ディスク 3 0 3 上のユーザに開放された記録領域であるユーザデータエリア（不図示）の物理セクタに対して、例えば、ある物理セクタ番号の物理セクタを基準として、シーケンシャルな論理セクタ番号の論理セクタが、順次割り当てられる。変換方法の事例

はINCITS T10 WORKING DRAFT “MultiMedia Command Set-4 (MMC-4)” に記述がある。

【0166】

LBAがPSNに変換されると、ステップS232の処理として、その変換されたPSNが指し示すディスク303上の位置が検索される。この検索の結果、ピックアップ（不図示）がディスク303上の、読み出すべき位置に移動されるなどの処理が実行され、ディスク303からセクタデータ351が読み出される。読み出されたセクタデータ351は、暗号化部312に供給される。

【0167】

暗号化部312には、認証処理部311からセッションキーKsが供給され、乱数発生部315から初期ベクトルIVも供給される。暗号化部312は、供給されたセッションキーKsと初期ベクトルIVを用いてセクタデータ351を暗号化する。暗号化されたセクタデータ351（この場合、Encrypted Sector Data #1）は、ステップS232の処理として、セクタ転送制御部313の制御のもと、ホスト302の復号部322に対して出力される。

【0168】

復号部322は、供給されたEncrypted Sector Data #1を、認証処理部321から供給されるセッションキーKsと、ドライブ装置301の乱数発生部315から供給された初期ベクトルIVを用いて復号し、セクタデータ361を生成する。このようにして生成されたセクタデータ361は、図示されていないアプリケーションソフトウェアやディスプレイやスピーカに提供される。

【0169】

このような処理がドライブ装置301とホスト302間で繰り返される。ドライブ装置301から、順次、Physical Sector Data が読み出される。すなわち、ディスク303側からは、ドライブ装置301の検索制御に応じて順次、連続的にセクタデータが読み出されドライブ装置301に供給される。

【0170】

ドライブ装置301は、ステップS233乃至S240の各ステップの処理において、順次、読み出したセクタデータを暗号化し、ホスト302の要求（リードコマンドの発行）に応じてホスト302に供給する。

【0171】

ドライブ装置301は、ホスト302に対してセクタデータを転送する際、セクタ転送カウンタ314により管理されているカウンタ値Nの更新処理なども行う。例えば、ステップS232の処理として、セクタデータ351が暗号化されてホスト302側に転送されると、セクタ転送カウンタ314のカウンタ値Nは、1だけ増加された値に更新される（ステップ47の処理）。よって、このようなカウンタ値Nの更新の処理が繰り返される（セクタデータが、順次、ホスト302側に転送されると）、カウンタ値Nの値が、閾値Nmaxよりも大きくなる（ $N > N_{max}$ を満たす）ときがある。

【0172】

図17を参照するに、 $(N1 + N2) < N_{max} < (N1 + N2 + N3)$ と設定されていたとする。このような場合、ステップS240において、 $(N1 + N2 + 1)$ 番目のセクタデータが出力された後の時点（セクタ転送カウンタ314が管理するカウンタ値Nが、 $(N1 + N2 + 1)$ となった後の時点）で、継続的に、セクタデータがディスク303から読み出され、暗号化され、転送されという処理が繰り返されると、カウンタ値Nの値は、順次1つずつ増加されるので、 $N > N_{max}$ という条件を満たすようになる。

【0173】

$N > N_{max}$ という条件が満たされると、すなわち、ステップS45（図13）において、YESと判断されると、ステップS48（図17においては、ステップS241）に処理が進められる。

【0174】

ステップ48（ステップS241）において、エラーメッセージ（Error Message）が

ドライブ装置 3 0 1 からホスト 3 0 2 側に出力される。ドライブ装置 3 0 1 のセクタ転送カウンタ 3 1 4 は、自己がカウントしているカウンタ値 N が、閾値 N_{\max} よりも大きくなったと判断したとき、セクタ転送制御部 3 1 3 に対して、暗号化部 3 1 2 から供給されるデータをホスト 3 0 1 側に出力しないように指示を出す。

【0 1 7 5】

セクタ転送制御部 3 1 3 は、セクタ転送カウンタ 3 1 4 から、出力停止の指示を受けると、セクタデータの出力を停止すると共に、メッセージ伝達部 3 1 6 に対して、出力停止の指示を受けたことを知らせる。メッセージ伝達部 3 1 6 は、セクタ転送制御部 3 1 3 から、出力停止の指示を受けたという知らせを受けると、エラーメッセージを作成し、ホスト 3 0 2 に対して送信する。このエラーメッセージは、ホスト 3 0 2 に、指示されたデータの供給はできないということを認識させるためのメッセージである。

【0 1 7 6】

このようなメッセージが出力されると、ドライブ装置 3 0 1 側からはデータが出力されない状態とされる。換言すれば、ドライブ装置 3 0 1 側で、認証処理が正常に行われた結果、データの出力が許可された状態であっても、その状態が解除され、許可されない状態に変更される。

【0 1 7 7】

このように、本実施の形態によれば、一度設定されたデータ出力の許可という状況を変更することが可能である。よって、エラーメッセージが出力された後、ホスト 3 0 2 から、ディスク 3 0 3 からのデータの読み出しが指示されても、その指示に対応して、データが読み出されることはない。

【0 1 7 8】

エラーメッセージが出力されると、ドライブ装置 3 0 1 からホスト 3 0 2 へのデータの出力が停止される。このようなデータの出力が停止されてしまような状況が発生しないようにするためには、ホスト 3 0 2 側で、初期ベクトル $I V$ の発行要求が、所定のタイミングでドライブ装置 3 0 1 に対して出されればよい。

【0 1 7 9】

すなわち、初期ベクトル $I V$ の発行が要求されれば（例えば、ステップ $S 4 0$ （図 1 3））、セクタ転送カウンタ 3 1 4 のカウンタ値 N が 0 にリセットされる（ステップ $S 4 2$ ）。その結果、 $N > N_{\max}$ という条件が満たされることを回避できるため、エラーメッセージが出力されるような状況が発生する（ステップ $S 4 8$ ）ようなことを回避することができる。

【0 1 8 0】

ホスト 3 0 2 は、定期的に初期ベクトル $I V$ の発行の要求を出す。定期的とは、例えば、初期ベクトル $I V$ の発行を要求した後、転送を指示したデータ量の累計が所定のデータ量（例えば、1 6 Mbyte（8 K Sector））を超える毎に要求されるということである。または、初期ベクトル $I V$ の発行を要求した後、所定の時間が経過する毎に要求されるということである。

【0 1 8 1】

いずれにしても、ホスト 3 0 2 は、所定のタイミングで、初期ベクトル $I V$ の発行の要求を出す。よって、正常に（正当に）処理が実行されている間、ドライブ装置 3 0 1 側では、ステップ $S 4 1$ 乃至 $S 4 3$ の処理が定期的に行われることになり、定期的にセクタ転送カウンタ 3 1 4 のカウンタ値 N が 0 に設定されることになる。

【0 1 8 2】

このようにすることで、少なくとも以下のような問題を解決することができる。

ドライブ装置 3 0 1 とホスト 3 0 2 との間で一旦、相互認証が成功したら、ドライブ装置 3 0 1 は、相手（ホスト 3 0 2 において起動されているアプリケーションなど）が正当であろうが、正当でなかろうが、保護されたデータを相手側の指示に従って出力してしまうといった問題。

バスを第 3 者が観測し、保護されたデータを横取りして解読し平文化してしまうといっ

た問題（不正に利用されてしまうという問題）。

【0183】

このような問題を解決するために、上述したように、まず、保護されたデータ（ディスク303に記録されているセクタデータ351）をドライブ装置301からホスト302にバス転送する際、その保護されたデータをセッションキーKsで暗号化してから転送するようにした。このことにより、仮に、バスを第3者が観測し、保護されたデータを横取りしたとしても、そのデータを解読し平文化することを困難にすることが可能となる。

【0184】

そして、データを暗号化する際、初期ベクトルIVを適用するようにした。またその初期ベクトルIVは、乱数を用いてランダムに変更されるようにした。このようにすることで、仮に、第3者が何らかの方法で、保護されたデータを横取りしたとしても、そのデータを解読し平文化することをより困難にすることが可能となる。

【0185】

また、初期ベクトルIVが変更されるようすることで、平文データが特別なデータであることを特定させることを困難にすることが可能となる。このことは、データのすり替えや、データの改竄など、不正な行為を防止できることを意味する。さらに、初期ベクトルIVを適宜更新させることで、大量のデータを単一の鍵で暗号化した場合に、暗号鍵（セッションキーKs）が予測されやすくなるといった問題を解決することが可能となる。

【0186】

また、上述したように、本実施の形態によれば、ホスト302側から適切に初期ベクトルIVの更新が指示されなければ、データの供給が停止されるため、ドライブ装置301とホスト302との間で一旦、相互認証が成功したら、ドライブ装置301は、相手（ホスト302において起動されているアプリケーションなど）が正当であろうが、正当でなかろうが、保護されたデータを相手側の指示に従って出力してしまうといった問題を解決することができる。

【0187】

すなわち、正当なドライブ装置301は、正当なホスト302にのみ、保護されたデータを転送するように制御することが可能となる。

【0188】

上述した実施の形態においては、初期ベクトルIVが更新されるとしたが、暗号化に用いられるセッションキーKs自体が更新されるようにしても良い。換言すれば、ホスト302からは、初期ベクトルIVの再発行の指示が出されるのではなく、セッションキーKsの再発行の処理が出されるようにしても良い。

【0189】

しかしながら、セッションキーKsは、相互認証が正常に終了されなければ生成されないため、セッションキーKsの更新に係る処理時間や処理能力を考慮すると、初期ベクトルIVの方を更新する方が好ましいと考えられる。

【0190】

上述した実施の形態においては、ディスク303からデータを読み出す（再生）の場合を例に挙げて説明したが、本発明はデータの再生にのみ適用範囲が限定されるわけではない。すなわち、本発明を、ディスク303へのデータの書き込み（記録）に適用することも可能である。

【0191】

図19は、本発明を記録装置に適用した場合のシステム構成例を示す図である。

【0192】

図19に示し記録装置のドライブ装置401は、ホスト402から供給されるデータを、セットされているディスク303に記録する。ドライブ装置401は、認証処理部411、復号部412、セクタ転送制御部413、セクタ転送カウンタ414、乱数発生部415、メッセージ伝達部416、コマンド処理部417、および、アクセス処理部418を含む構成とされている。

【0193】

ホスト402は、認証処理部421、暗号化部422を含む構成とされている。

【0194】

図19に示した記録装置の構成は、図10に示した再生装置の構成と同様な部分が多いので、その詳細な説明は省略し、異なる部分についてのみ説明を加える。

【0195】

図19に示した記録装置は、ディスク403にセクタデータを451を記録する。この記録されるセクタデータ451は、ホスト402側から供給されるセクタデータ461である。ホスト402の暗号化部422は、図示されていない記録媒体またはハードディスクドライブなどから読み出されたセクタデータ461を、認証処理部421から供給されるセッションキーKsを用いて暗号化する。

【0196】

暗号化部422により暗号化されたセクタデータ461は、ドライブ装置401のセクタ転送制御部413に供給される。セクタ転送制御部413は、供給されたセクタデータ461を、復号部412に供給する。復号部412は、供給されたセクタデータ461を、認証処理部411から供給されるセッションキーKsを用いて復号する。復号されたセクタデータ461は、セクタデータ451として、アクセス処理部418の制御のもと、ディスク403に記録される。

【0197】

セクタ転送カウンタ414は、セクタ転送制御部413から出力され、復号部412に供給されたセクタ数をカウントする。その他の部分に関しては、図10に示した再生装置の対応する部分と、基本的に同様な構成であり、その動作も同様である。

【0198】

図19に示した記録装置のドライブ装置401は、既に図12、図13のフローチャートを参照して説明した処理と、基本的に同様な処理を実行するため、詳細な説明は省略する。ここでは、再度、図12、図13のフローチャートを参照し、異なる処理のみに説明を加える。

【0199】

ドライブ装置401は、ステップS44において、セクタデータの記録の要求があったか否かを判断する。この判断は、コマンド処理部417が、ホスト402側から、コマンドパケット463を受信したか否かを判断し、かつ、受信したコマンドパケット463が、セクタデータ461の書き込みを要求するもの（すなわち、ライトコマンド）であるか否かを判断することにより行われる。

【0200】

また、ステップS46においては、暗号化されたセクタデータ461が供給されるため、復号部412における復号処理が行われ、その復号されたセクタデータ461（451）がディスク403に書き込まれる処理が実行される。その他の処理については、基本的に同様であり、ホスト402から定期的に初期ベクトルIVの発行要求が出されなければ、ドライブ装置401側における書き込みの処理が停止される（ホスト403からのデータの出力が停止される）ように制御される。

【0201】

よって、ホスト402側で管理している保護されたデータが、不正に出力されること、そして、ディスク403に書き込まれてしまふことを防ぐことが可能となる。

【0202】

図20のタイミングチャートを参照して、図19に示した記録装置における、データの記録に関わる処理について説明を加えるが、基本的な処理は、図17に示したタイミングチャートと同様であるので、その詳細な説明は省略する。異なる処理としては、ステップS301において、ホスト402から、データの書き込みを指示するライトコマンド（WRITE command）が送信される。

【0203】

また、ステップ S 3 0 2 において、ホスト 4 0 2 の暗号化部 4 2 2 は、セクタデータ 4 6 1 をセッションキー Ks を用いて暗号化し、その暗号化したデータ (Encrypted Sector Data # 1) を、ドライブ装置 4 0 1 に対して送信する。ドライブ装置 4 0 1 のセクタ転送制御部 4 2 3 は、供給された Encrypted Sector Data # 1 を、復号部 4 1 2 に供給する。

【0204】

復号部 4 1 2 は、認証処理部 4 1 1 から供給されるセッションキー Ks と、乱数発生部 4 1 5 から供給された初期ベクトル I V を用いて復号し、セクタデータ 4 5 1 を生成する。このようにして生成されたセクタデータ 4 5 1 は、アクセス処理部 4 1 8 の制御に基づき、ディスク 4 0 3 に書き込まれる。

【0205】

このような処理が行われると共に、セクタ転送カウンタ 4 1 4 は、セクタ転送制御部 4 1 3 から出力されたセクタ数をカウントする。そして、そのカウントされているカウンタ値 N が、 N_{max} 以上になったか否かの判断を行う。カウンタ値 N が大きくなると、すなわち、セクタデータが、順次、セクタ転送制御部 4 1 3 から出力されると、カウンタ値 N の値が、閾値 N_{max} よりも大きくなる ($N > N_{max}$ を満たす) ときがある。

【0206】

図 20 を参照するに、 $(N_1 + N_2) < N_{max} < (N_1 + N_2 + N_3)$ と設定されていたとする。このような場合、ステップ S 3 4 0 において、 $(N_1 + N_2 + 1)$ 番目のセクタデータが受信された後の時点 (セクタ転送カウンタ 4 1 4 が管理するカウンタ値 N が、 $(N_1 + N_2 + 1)$ となった後の時点) で、継続的に、セクタデータがディスク 4 0 3 に書き込まれるという処理が繰り返されると、カウンタ値 N の値は、順次 1 つづ増加されるので、 $N > N_{max}$ という条件を満たすようになる。

【0207】

$N > N_{max}$ という条件が満たされると、すなわち、ステップ S 4 5 (図 13) において、YES と判断されると、ステップ S 4 8 (図 20 においては、ステップ S 3 4 1) に処理が進められる。

【0208】

ステップ 4 8 (ステップ S 3 4 1) において、エラーメッセージ (Error Message) がドライブ装置 4 0 1 からホスト 4 0 2 側に出力される。ドライブ装置 4 0 1 のセクタ転送カウンタ 4 1 4 は、自己がカウントしているカウンタ値 N が、閾値 N_{max} よりも大きくなったと判断したとき、セクタ転送制御部 4 1 3 に対して、復号部 4 1 2 にデータを出力しないように指示を出す。

【0209】

セクタ転送制御部 4 1 3 は、セクタ転送カウンタ 4 1 4 から、出力停止の指示を受けると、セクタデータの出力を停止すると共に、メッセージ伝達部 4 1 6 に対して、出力停止の指示を受けたことを知らせる。メッセージ伝達部 4 1 6 は、セクタ転送制御部 4 1 3 から、出力停止の指示を受けたという知らせを受けると、エラーメッセージを作成し、ホスト 4 0 2 に対して送信する。このエラーメッセージは、ホスト 4 0 2 に、指示されたデータの書き込みはできないということを認識させるためのメッセージである。

【0210】

このようなメッセージが出力されると、ドライブ装置 4 0 1 側からはデータが入力されない状態とされる。また、エラーメッセージを受け取ったホスト 4 0 2 は、データを出力しない状態とされる。

【0211】

このように処理が行われることで、既に説明した再生装置の場合と同様の効果を望むことが可能である。

【0212】

このように、本発明を適用することにより、ドライブ装置とホストとの間で行われるデータの授受に関し、セキュリティを向上させることが可能となる。

【0213】

なお、上述した実施の形態においては、再生装置（図10）と記録装置（図19）をそれぞれ別な構成として図示および説明したが、再生装置と記録装置を同一の装置内に納めることも可能である。同一の装置内に納めるようにした場合、再生装置内と記録装置内において同一の処理を実行する、例えば、乱数発生部315（415）などは、再生装置と記録装置で共用される構成としても、もちろん良い。

【0214】

なお、上述した実施の形態においては、暗号化および復号の方式として、CBC方式を例に挙げて説明したが、本発明は、CBC方式にのみ適用できることを示すものではない。例えば、CFB（Cipher Feed Back）方式、OFB（Output Feed Block）方式などに対しても本発明を適用することはできる。

【実施例2】

【0215】

実施例1においては、ドライブ装置301（401）側で初期ベクトルIVを生成する場合を例にあげて説明したが、実施例2とし、ホスト側で初期ベクトルIVを生成する場合について説明する。

【0216】

図21は、実施例2におけるシステムの構成を示す図である。ドライブ装置501は、認証処理部511、復号部512、入力制御部513、セクタ転送カウンタ514、リセット処理部515、メッセージ伝達部516、コマンド処理部517、および、アクセス処理部518を含む構成とされている。

【0217】

ホスト502は、認証処理部521、暗号化部522、セクタ転送カウンタ523、乱数発生部524、および、スイッチ525を含む構成とされている。

【0218】

図21に示したシステムにおいては、ホスト502からドライブ装置501に対して、暗号化された状態のセクタデータ561が供給され、そのセクタデータ561が、復号された後に、セクタデータ551としてディスク503に書き込まれる。

【0219】

ドライブ装置501の認証処理部511とホスト502の認証処理部521により、相互認証に関わる処理が実行される。

【0220】

ホスト502の暗号化部522には、ディスク503に書き込まれるセクタデータ561と、認証処理部511からセッションキーKsが供給される。また、暗号化部522には、乱数発生部524により発生された乱数が、初期ベクトルIVとして供給される。暗号化部522は、供給されたセクタデータ561をセッションキーKsと初期ベクトルIVを用いて暗号化し、ドライブ装置501に送信する。

【0221】

ドライブ装置501の入力制御部513は、ホスト502から、暗号化されたセクタデータ561を入力した場合、復号部512に転送する。復号部512には、ホスト502から、セクタデータ561とは別の経路で、乱数発生部524により発生された初期ベクトルIVも供給される。

【0222】

復号部512は、認証処理部511から供給されるセッションキーKsと、ホスト502から供給される初期ベクトルIVを用いて復号処理を実行し、セクタデータ551（セクタデータ561と同一のデータ）を生成する。生成されたセクタデータ551は、ディスク503に書き込まれる。この書き込みは、アクセス処理部518の制御のもと行われる。

【0223】

ホスト502は、セクタデータ561を出力する際、セクタ転送カウンタ523により、転送する（転送した）セクタ数をカウントするように構成されている。そして、そのカ

ウント数に応じ、スイッチ 525 を切り換えるように構成されている。詳細は後述するが、カウント数（以下、適宜、カウント値 N とする）が、所定の数（以下、適宜、閾値 N_{max} とする）に達する前の時点で、センドキーコマンド 563 により、初期ベクトル $I V$ を転送するように構成されている。

【0224】

同様に、ドライブ装置 501 側にも、セクタ転送カウンタ 514 が設けられている。セクタ転送カウンタ 514 は、入力制御部 513 から復号部 512 に供給されたセクタ数をカウントしている。セクタ転送カウンタ 514 は、カウント数（以下、適宜、カウント値 M とする）が所定の数（以下、適宜、閾値 M_{max} とする）に達した場合、入力制御部 513 にセクタデータを入力しないように指示を出すとともに、メッセージ伝達部 516 に対してメッセージの伝達を指示する。

【0225】

なお、ホスト 502 のセクタ転送カウンタ 523 に設定されている閾値 N_{max} は、ドライブ装置 514 のセクタ転送カウンタ 514 に設定されている閾値 M_{max} よりも小さい値とされている（ $N_{max} < M_{max}$ という条件を満たす値とされている）。

【0226】

また、ここでは、セクタ転送カウンタ 514 は、カウント値 M が閾値 M_{max} に達した場合、入力制御部 513 にセクタデータを入力しないように指示を出すとして説明を続けるが、入力制御部 513 に、入力されたセクタデータを復号部 512 に転送しないように指示を出すようにしても良い。

【0227】

セクタ転送カウンタ 514 のカウント値 M をリセットする（0 にする）ために、リセット処理部 515 が設けられている。リセット処理部 515 に対する指示は、コマンド処理部 517 により出される。

【0228】

このような構成を有するシステムにより行われる処理について説明する。まず、図 22 のタイミングチャートを参照して、初期ベクトル $I V$ に係る処理について説明する。ホスト 502 は、ステップ $S 501$ において、ドライブ装置 501 は、ステップ $S 521$ において、それぞれ相互認証（Authentication）を行う。この相互認証が正常に行われた場合のみ、次のステップに処理が進められる。また、この相互認証の結果、ドライブ装置 501 の認証処理部 511 とホスト 502 の認証処理部 521 との、それぞれにおいてセッションキー K_s が生成される（共有される）ことになる。

【0229】

ホスト 502 は、ステップ $S 502$ において、センドキーコマンド（SEND KEY command）563 を生成し、ドライブ装置 501 に対して出力する。ステップ $S 502$ において生成され、出力されるセンドキーコマンド 563 は、初期ベクトル $I V$ の転送するためのものである。

【0230】

ステップ $S 503$ において、初期ベクトル $I V$ が生成され、転送される。この初期ベクトル $I V$ は、センドキーコマンド 563 により転送される。ドライブ装置 501 は、ステップ $S 522$ 、 $S 523$ により、センドキーコマンド 563 および初期ベクトル $I V$ を受信する。コマンド処理部 517 は、受信したセンドキーコマンド 563 を、リセット処理部 515 に供給する。

【0231】

リセット処理部 515 は、センドキーコマンド 563 が供給された場合、セクタ転送カウンタ 514 に対して、カウント値 M をリセットするように（0 に戻すように）指示を出す。また、センドキーコマンド 563 に含まれる初期ベクトル $I V$ は、復号部 512 に供給される。

【0232】

このようにして、ドライブ装置 501 とホスト 502 の両方で、共通のセッションキー

Ksと初期ベクトルIVが共用される。共通のセッションキーKsと初期ベクトルIVが共用された後の処理について、図23のタイミングチャートを参照して説明する。

【0233】

ステップS551において、ホスト502から、セクタデータの書き込みを指示するライトコマンド(WRITE command)が送信される。また、ステップS552において、ホスト502の暗号化部522は、セクタデータ561をセッションキーKsと初期ベクトルIVを用いて暗号化し、その暗号化したデータ(Bus-Encrypted Sector Data)を、ドライブ装置501に対して送信する。ドライブ装置501の入力制御部513は、供給されたBus-Encrypted Sector Dataを、復号部512に供給する。

【0234】

復号部512は、認証処理部511から供給されるセッションキーKsと、乱数発生部524により発生され、供給された初期ベクトルIVを用いて復号し、セクタデータ551を生成する。このようにして生成されたセクタデータ551は、アクセス処理部518の制御に基づき、ディスク503に書き込まれる。

【0235】

このような処理が行われると共に、ホスト502側のセクタ転送カウンタ523は、送信されたセクタ数をカウントする。そして、そのカウントされているカウンタ値Nが、Nmax以上になったか否かの判断を行う。カウンタ値Nが大きくなると、すなわち、セクタデータが、順次、送信されると、カウンタ値Nの値が、閾値Nmaxよりも大きくなる(N > Nmaxを満たす)ときがある。

【0236】

そのような状況になると、ホスト502からは、センドキーコマンド563が送信される。図23のタイミングチャートにおいては、ステップS555のタイミングでセンドキーコマンド563が送信されている。

【0237】

ホスト502から送信されたセンドキーコマンド563は、ステップS585においてドライブ装置501に受信される。ドライブ装置501のセクタ転送カウンタ514は、センドキーコマンド563が受信されたことによりリセットされる。よって、ホスト502から適切なタイミングでセンドキーコマンド563が出力されている間は、セクタ転送カウンタ514によるカウント値Mが閾値Mmax以上になることはないため、入力制御部513によりデータの入力が拒否されるような状況が発生するようなことがないため、ディスク503へのセクタデータの書き込みは継続的に行われることになる。

【0238】

次に、ドライブ装置501とホスト502の、それぞれの処理について説明を加える。図24と図25のフローチャートを参照して、ホスト502側の処理について説明する。ホスト502は、ステップS601において、所定のアプリケーションが起動されているか否かを判断する。所定のアプリケーションとは、ここでは、ドライブ装置501に挿入されたディスク503に対してデータを書き込むために必要とされるアプリケーションである。

【0239】

ステップS601において、アプリケーションは起動されていると判断された場合、ステップS602において、ドライブ装置501にディスク503が、挿入されているか否かが判断される。ステップS602において、ドライブ装置501にディスク503が挿入されていると判断された場合、ステップS503に処理が進められ、ドライブ装置501とホスト502との間で相互認証処理が実行され、セッションキーKsが、ドライブ装置501とホスト502で、それぞれ生成(共用)される。

【0240】

ステップS604において、セッションキーKsの生成が完了したか否かが判断される。セッションキーKsの生成が完了されるまで、ステップS603とステップS604の処理が繰り返される。

【0241】

そして、ステップS604において、セッションキーKsの生成が完了したと判断されると、ステップS605に処理が進められ、初期ベクトルIVが生成される。そして、ステップS606において、センドキーコマンド563が生成される。このようにして生成されたセンドキーコマンド563を用いて、初期ベクトルIVが、ステップS607の処理としてドライブ装置501側に送信される。

【0242】

ステップS608において、セクタ転送カウンタ523のカウント値Nが0にセットされる。ステップS609（図25）において、ライトコマンド（WRITE command）を送信するか否かが判断される。ライトコマンドではなく他のコマンドを送信すると判断された場合、ステップS610において、他のコマンドに対する処理が実行される。

【0243】

一方、ステップS609において、ライトコマンドを送信すると判断された場合、ステップS611において、セクタ転送カウンタ523によりカウントされているカウント値Nが、 $N+L$ に更新される。このLは、ライトコマンドに含まれるTransfer Lengthの部分に書き込まれている数値である。このTransfer Lengthは、上述したように書き込みセクタ数を指示するデータであるため、Lが示す値は、その時点に送信されるセクタデータ数に対応していることになる。

【0244】

ステップS612において、セクタ転送カウンタ523によりカウントされているカウント値Nが、閾値Nmaxよりも大きくなったか否か（ $N > N_{max}$ の条件を満たすか否か）が判断される。ステップS612において、 $N > N_{max}$ の条件を満たすと判断された場合、ステップS613に処理が進められる。 $N > N_{max}$ の条件を満たす状況とは、ここでは、センドキーコマンド563や初期ベクトルIVを送信する（更新する）タイミングであることを示している。

【0245】

ステップS613乃至S616の処理は、ステップS606乃至S608の処理と同様である。すなわち、センドキーコマンド563や初期ベクトルIVが新たに生成され、ドライブ装置501側に送信される処理である。

【0246】

一方、ステップS612において、 $N > N_{max}$ の条件を満たさないと判断された場合、ステップS617に処理が進められ、ライトコマンドが生成され、送信される。そして、ステップS618において、セクタデータ561が、暗号化部522により暗号化され、その暗号化されたセクタデータ561が、ドライブ装置501側に送信される。

【0247】

このような処理が、ホスト502側で行われる一方で、ドライブ装置501側では、図26、図27に示すフローチャートの処理が実行される。

【0248】

ドライブ装置501は、ステップS631において、ディスク503が挿入されているか否かを判断する。ステップS631において、ドライブ装置501にディスク503が挿入されていると判断された場合、ステップS632に処理が進められる。ステップS632において、ホスト502側で所定のアプリケーションが起動されているか否かが判断される。

【0249】

ステップS632において、アプリケーションは起動されていると判断された場合、ステップS633において、ドライブ装置501とホスト502との間で相互認証処理が実行され、セッションキーKsが、ドライブ装置501とホスト502で、それぞれ生成（共用）される。

【0250】

ステップS634において、セッションキーKsの生成が完了したか否かが判断される

。セッションキー K_s の生成が完了されるまで、ステップ S 6 3 3 とステップ S 6 3 4 の処理が繰り返される。そして、ステップ S 6 3 4 において、セッションキー K_s の生成が完了したと判断されると、ステップ S 6 3 5 に処理が進められる。

【0251】

ステップ S 6 3 5 において、セクタ転送カウンタ 5 1 4 のカウンタ値 M が閾値 M_{max} に設定される。このように、 $M = M_{max}$ に設定されると、セクタ転送カウンタ 5 1 4 の指示により、入力制御部 5 1 3 でホスト 5 0 2 からのデータの inputs が許可されない状態に設定される。

【0252】

ステップ S 6 3 6 (図 2 7) において、センドキーコマンド (SEND KEY command) 5 6 3 を受信したか否かが判断され、受信したと判断された場合、ステップ S 6 3 7 に処理が進められる。ステップ S 6 3 7 において、センドキーコマンド 5 6 3 により送信されてきた初期ベクトル I_V が受信される。センドキーコマンド 5 6 3 が受信されることで、リセット処理部 5 1 5 から、セクタ転送カウンタ 5 1 4 に対して、カウンタ数 M を 0 にリセットするように指示が出される。

【0253】

このような指示を受け取ったセクタ転送カウンタ 5 1 4 は、ステップ S 6 3 8 の処理として、カウンタ値 M を 0 にリセットする。このようにセクタ転送カウンタ 5 1 4 のカウンタ値 M が、0 に設定される (閾値 M_{max} 以下の状態にされる) ことにより、入力制御部 6 1 3 へのデータの inputs が許可された状態にされる。

【0254】

ステップ S 6 3 9 において、初期ベクトル I_V が、復号部 5 1 2 に供給される。ステップ S 6 4 0 において、ライトコマンド 5 6 4 を受信したか否かが判断され、受信していないと判断されると、ステップ S 6 3 6 に戻り、それ以降の処理が繰り返される。一方、ステップ S 6 4 0 において、ライトコマンド 5 6 4 を受信したと判断した場合、ステップ S 6 4 1 に処理が進められる。

【0255】

ステップ S 6 4 1 において、セクタ転送カウンタ 5 1 4 のカウンタ値 M に Transfer Length の値 L を加算した値 ($M + L$) が、閾値 M_{max} 以上であるか否か ($M + L > M_{max}$ という条件を満たすか否か) が判断される。ステップ S 6 4 1 において、 $M + L > M_{max}$ という条件は満たされていないと判断された場合、ステップ S 6 4 2 に処理が進められ、カウンタ値 M が $M + L$ に更新される。 $M + L > M_{max}$ という条件が満たされていない状況とは、入力制御部 5 1 3 においてデータの inputs が許可された状態を示す。

【0256】

ステップ S 6 4 3 において、暗号化されているセクタデータ 5 6 1 が受信される。そして、受信されたセクタデータ 5 6 1 は、復号部 5 1 2 において復号され、セクタデータ 5 5 1 として、ディスク 5 0 3 に書き込まれる。

【0257】

一方、ステップ S 6 4 1 において、 $M + L > M_{max}$ という条件を満たすと判断された場合、ステップ S 6 4 4 に処理が進められる。 $M + L > M_{max}$ という条件が満たされる状態になると、セクタ転送カウンタ 5 1 4 から入力制御部 5 1 3 に対してセクタデータの inputs の停止が指示されるとともに、メッセージ伝達部 5 1 6 に対してメッセージの送信が指示される。

【0258】

メッセージ伝達部 5 1 6 から送信されるメッセージは、セクタデータの inputs を許可しない (従って、ディスク 5 0 3 へのセクタデータの書き込みを許可しない) ということをホスト 5 0 2 に認識させるためのエラーメッセージである。ステップ S 6 4 4 において、エラーメッセージが送信された後、ステップ S 6 3 6 に処理が戻され、それ以降の処理が繰り返される。

【0259】

このようなエラーメッセージが出されることにより、ホスト502がドライブ装置501の状態を認識し、センドキーコマンドを発行し、初期ベクトルI Vを供給すれば、すなわち、ステップS636において、センドキーコマンドを受信したと判断されれば、ステップS637以降に処理が進められるので、再度、セクタデータの入力が許可された状態に設定し直される。

【0260】

このように、ホスト502側で、初期ベクトルI Vを生成し、また、その初期ベクトルI Vの有効期間（寿命）を管理できるようにすることで、ドライブ装置とホストとの間で行われるデータの授受に関し、セキュリティを向上させることが可能となる。

【0261】

また、実施例2のようにした場合においても、実施例1の場合と同様な効果を得ることが可能である。

【0262】

上述した一連の処理は、それぞれの機能を有するハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、記録媒体からインストールされる。

【0263】

記録媒体は、その記録媒体を扱うパーソナルコンピュータとは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク（フレキシブルディスクを含む）、光ディスク（CD-ROM（Compact Disc-Read Only Memory）、DVD（Digital Versatile Disc）を含む）、光磁気ディスク（MD（Mini-Disc）（登録商標）を含む）、若しくは半導体メモリなどよりなるパッケージメディアにより構成されるだけでなく、コンピュータに予め組み込まれた状態でユーザに提供される、プログラムが記憶されているROMやハードディスクなどで構成される。

【0264】

なお、本明細書において、媒体により提供されるプログラムを記述するステップは、記載された順序に従って、時系列的に行われる処理は勿論、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0265】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【図面の簡単な説明】

【0266】

- 【図1】従来の再生装置の一例の構成を示す図である。
- 【図2】従来の再生装置の他の構成例を示す図である。
- 【図3】認証処理について説明するためのフローチャートである。
- 【図4】暗号化を行う回路の構成例を示す図である。
- 【図5】復号を行う回路の構成例を示す図である。
- 【図6】従来の再生装置における問題点を説明するための図である。
- 【図7】従来の再生装置における問題点を説明するための図である。
- 【図8】初期ベクトルI Vを授受する際の問題点を説明するための図である。
- 【図9】初期ベクトルI Vを授受する際の問題点を説明するための図である。
- 【図10】本発明を適用したシステムの一実施の形態の構成を示す図である。
- 【図11】データの授受に係わるドライバーについて説明するための図である。
- 【図12】ドライブ装置の動作について説明するためのフローチャートである。
- 【図13】図12のフローチャートに続くフローチャートである。
- 【図14】初期ベクトルI Vの授受に関するタイミングチャートである。

- 【図 1 5】 初期ベクトル I V の授受に関するタイミングチャートである。
【図 1 6】 初期ベクトル I V の授受に関するタイミングチャートである。
【図 1 7】 データの授受に関するタイミングチャートである。
【図 1 8】 コマンドパケットの構成を示す図である。
【図 1 9】 本発明を適用したシステムの他の実施の形態の構成を示す図である。
【図 2 0】 データの授受に関するタイミングチャートである。
【図 2 1】 実施例 2 における記録装置の構成を示す図である。
【図 2 2】 初期ベクトル I V の授受に関するタイミングチャートである。
【図 2 3】 初期ベクトル I V の授受に関するタイミングチャートである。
【図 2 4】 ホストの動作について説明するためのフローチャートである。
【図 2 5】 図 2 4 のフローチャートに続くフローチャートである。
【図 2 6】 ドライブ装置の動作について説明するためのフローチャートである。
【図 2 7】 図 2 6 のフローチャートに続くフローチャートである。

【符号の説明】

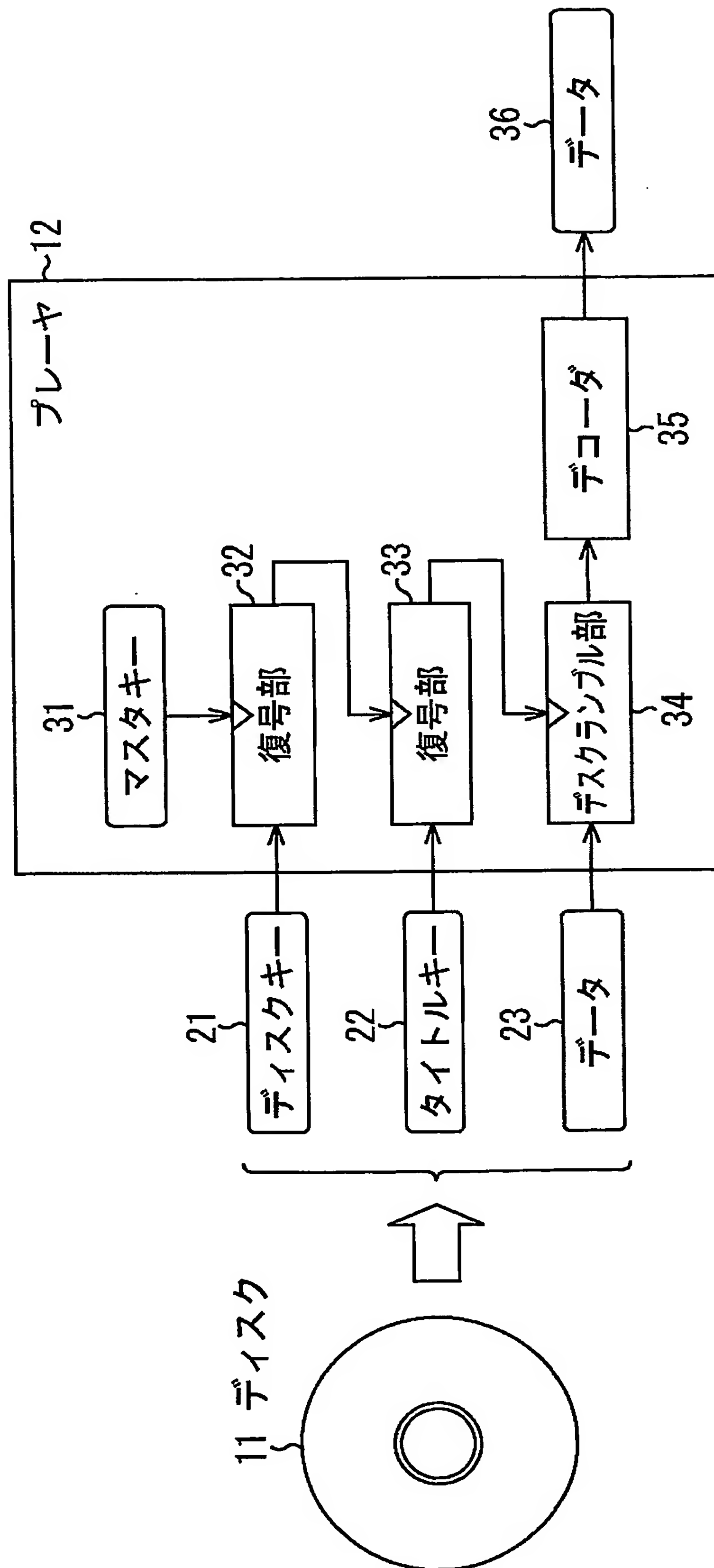
【 0 2 6 7 】

3 0 1 ドライブ装置, 3 0 2 ホスト, 3 0 3 ディスク, 3 1 1 認証処理部,
3 1 2 暗号化部, 3 1 3 セクタ転送制御部, 3 1 4 セクタ転送カウンタ,
, 3 1 5 乱数発生部, 3 1 6 メッセージ伝達部, 3 1 7 コマンド処理部,
3 1 8 アクセス処理部, 3 2 1 認証処理部、 3 2 2 復号部, 4 0 1 ドライブ装置,
4 0 2 ホスト, 4 0 3 ディスク, 4 1 1 認証処理部, 4 1 2 復号部,
4 1 3 セクタ転送制御部, 4 1 4 セクタ転送カウンタ, 4 1 5 乱数発生部,
4 1 6 メッセージ伝達部, 4 1 7 コマンド処理部, 4 1 8 アクセス処理部,
4 2 1 認証処理部、 4 2 2 暗号化部

【書類名】 図面

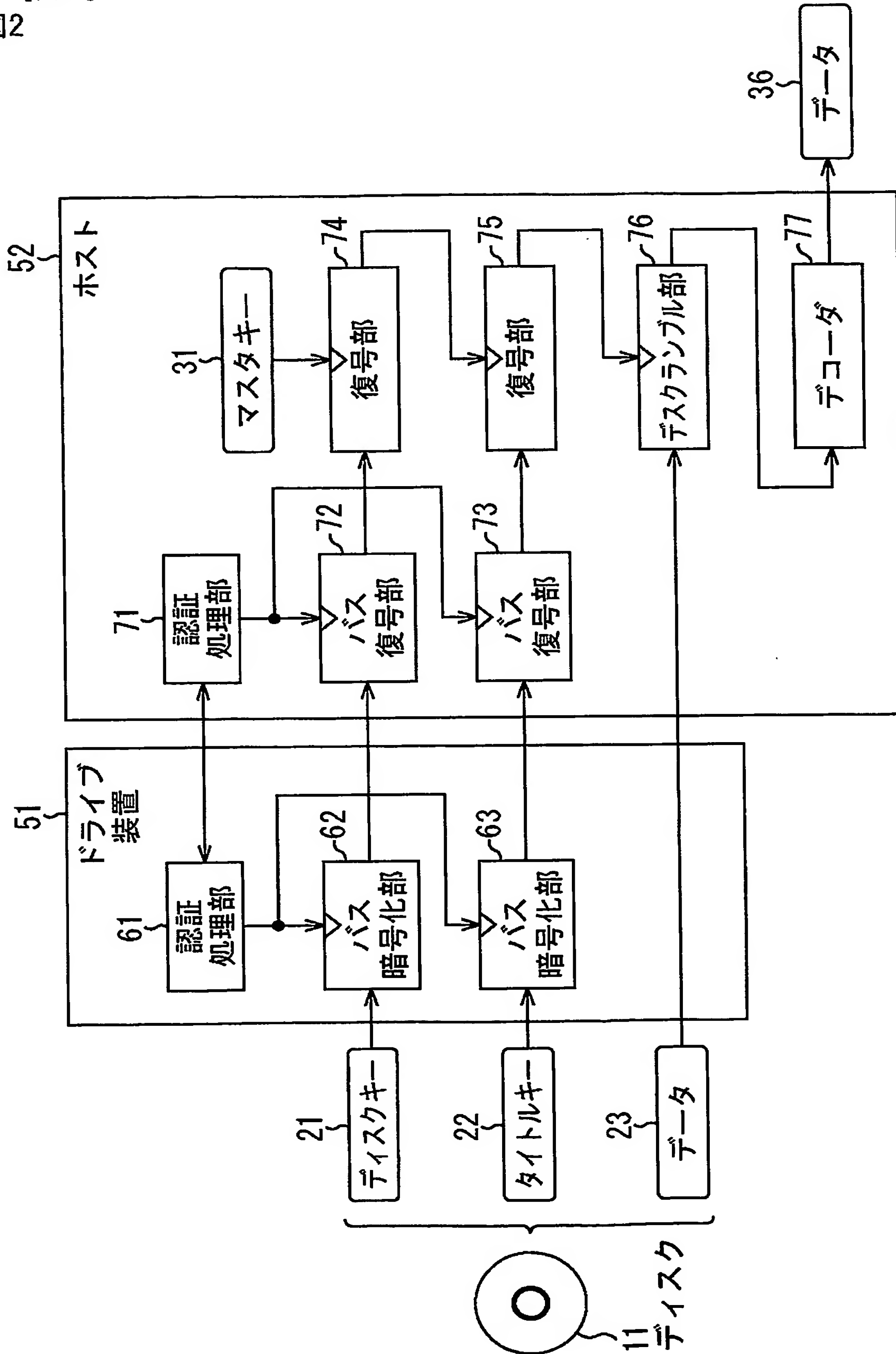
【図 1】

图 1



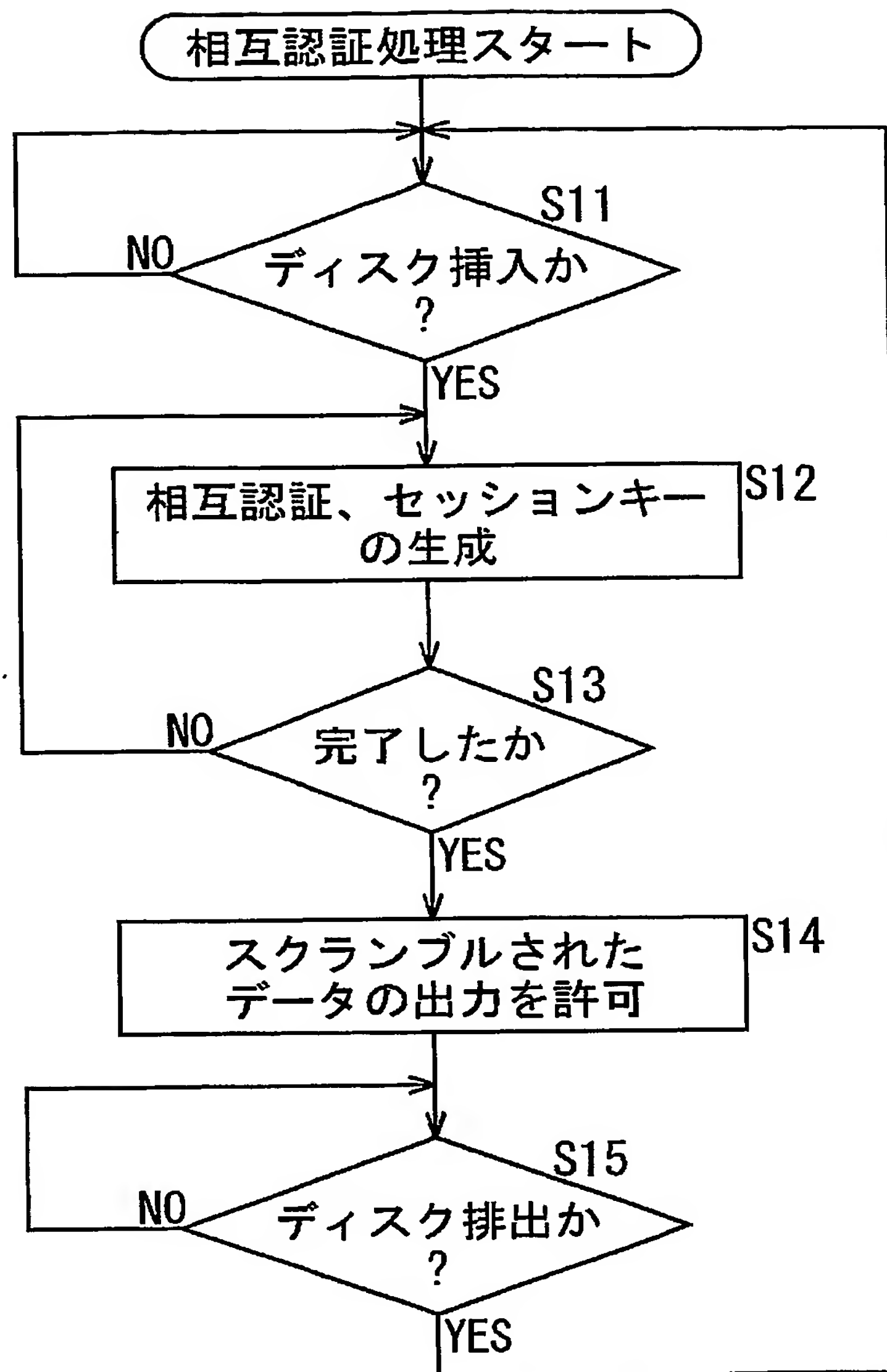
【図2】

図2



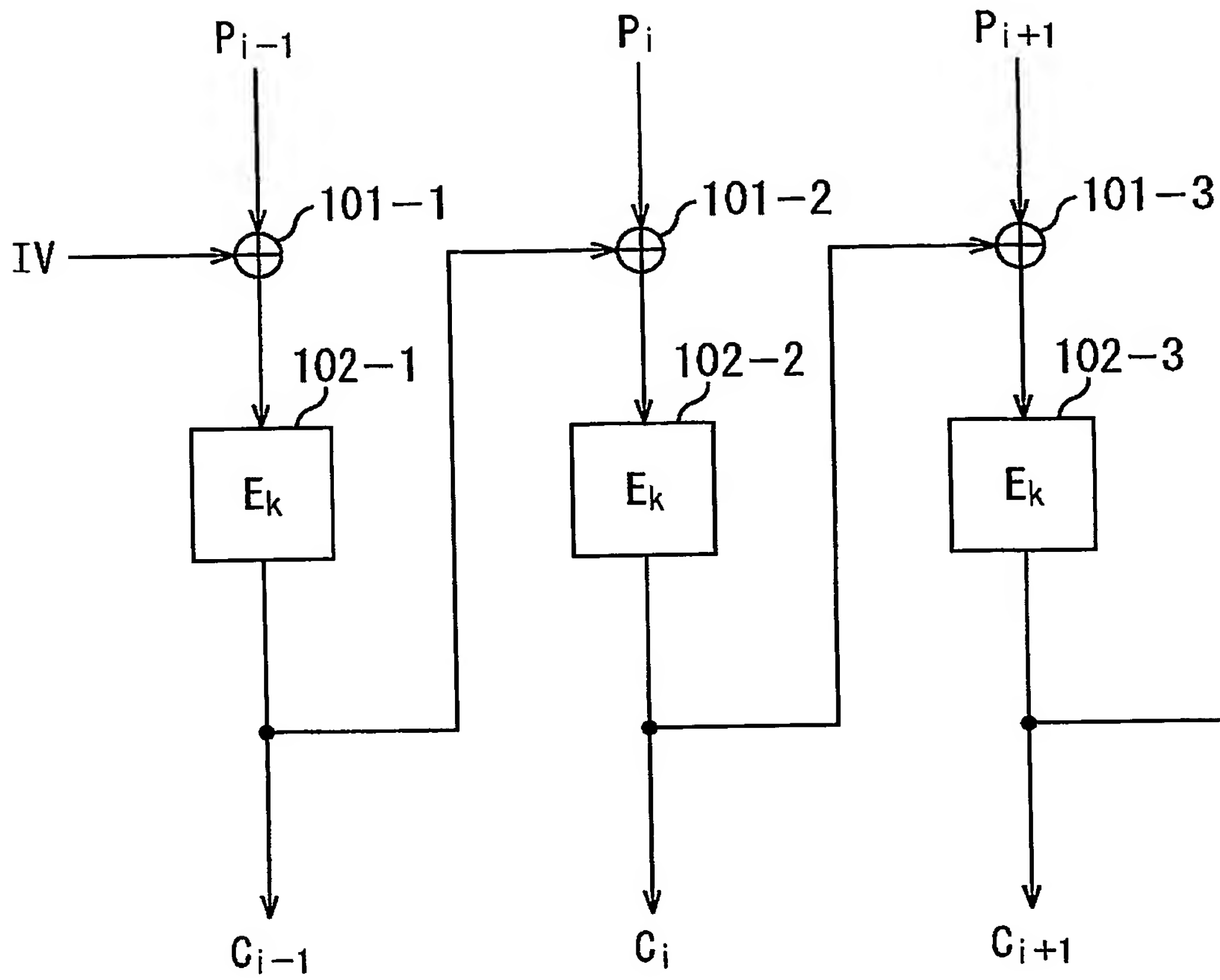
【図 3】

図3

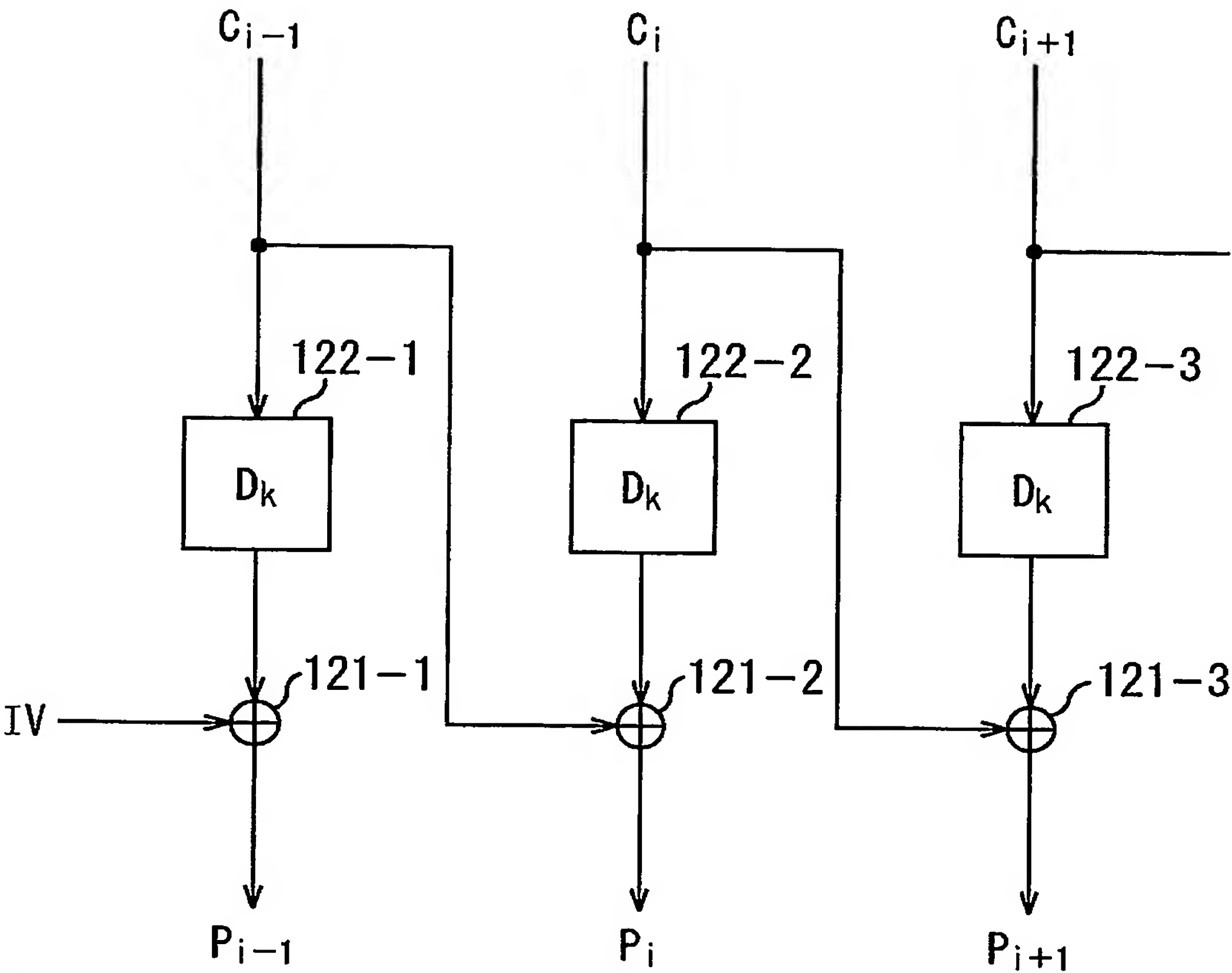


【図 4】

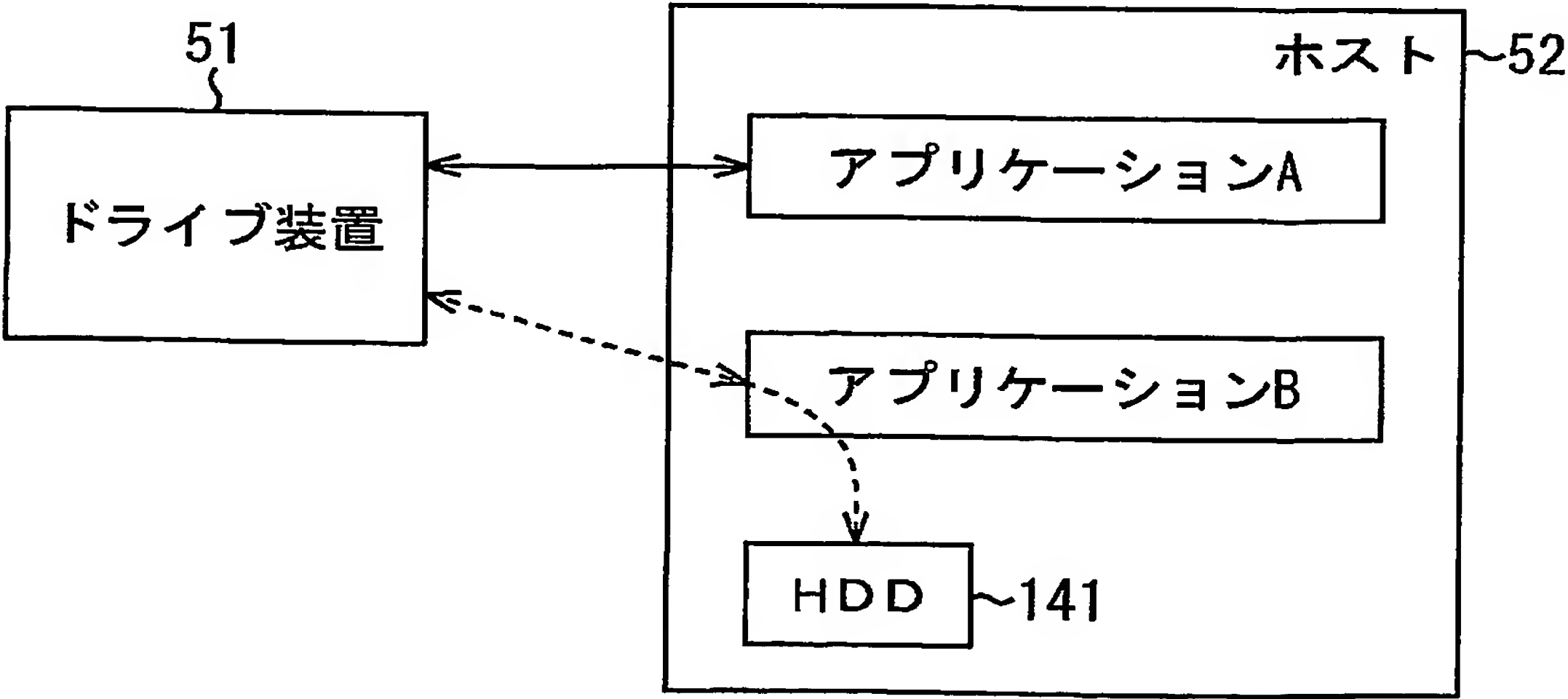
図4



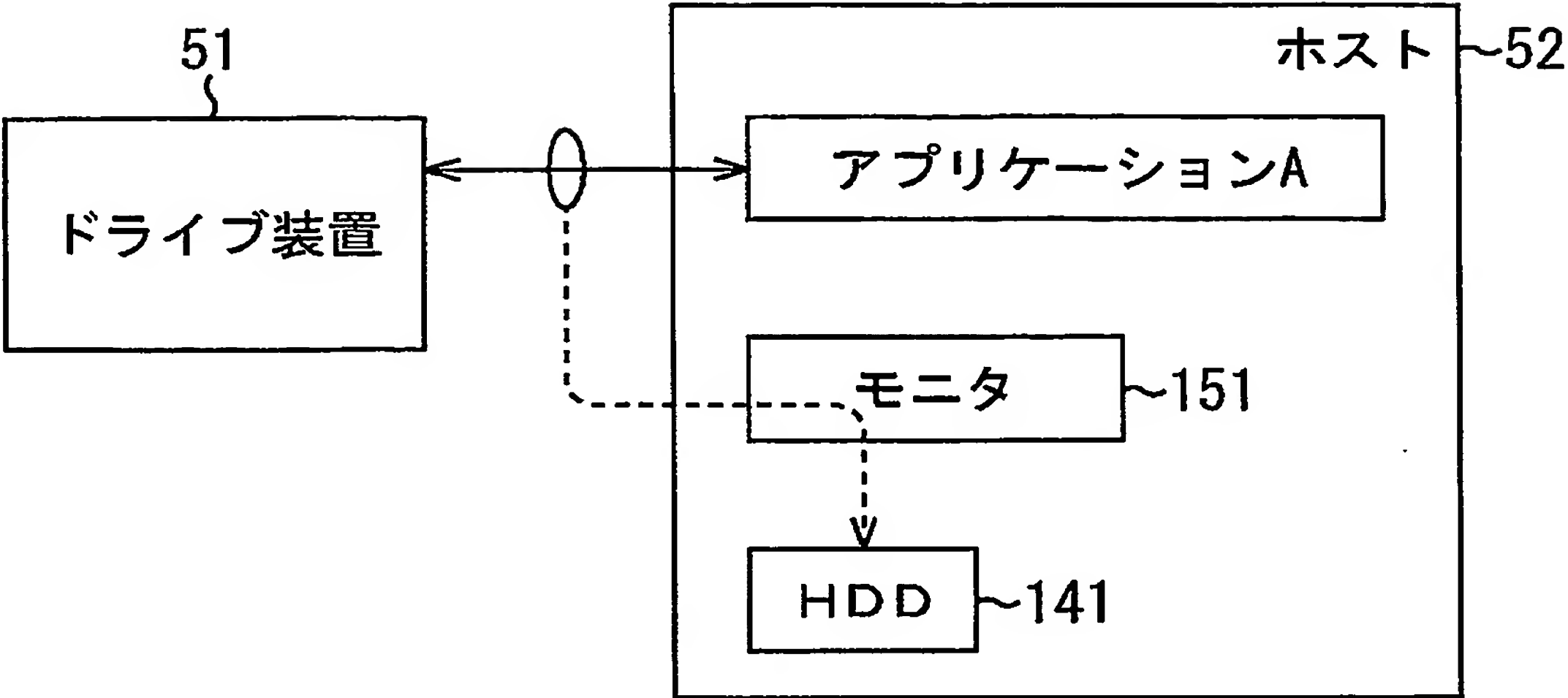
【図 5】
図5



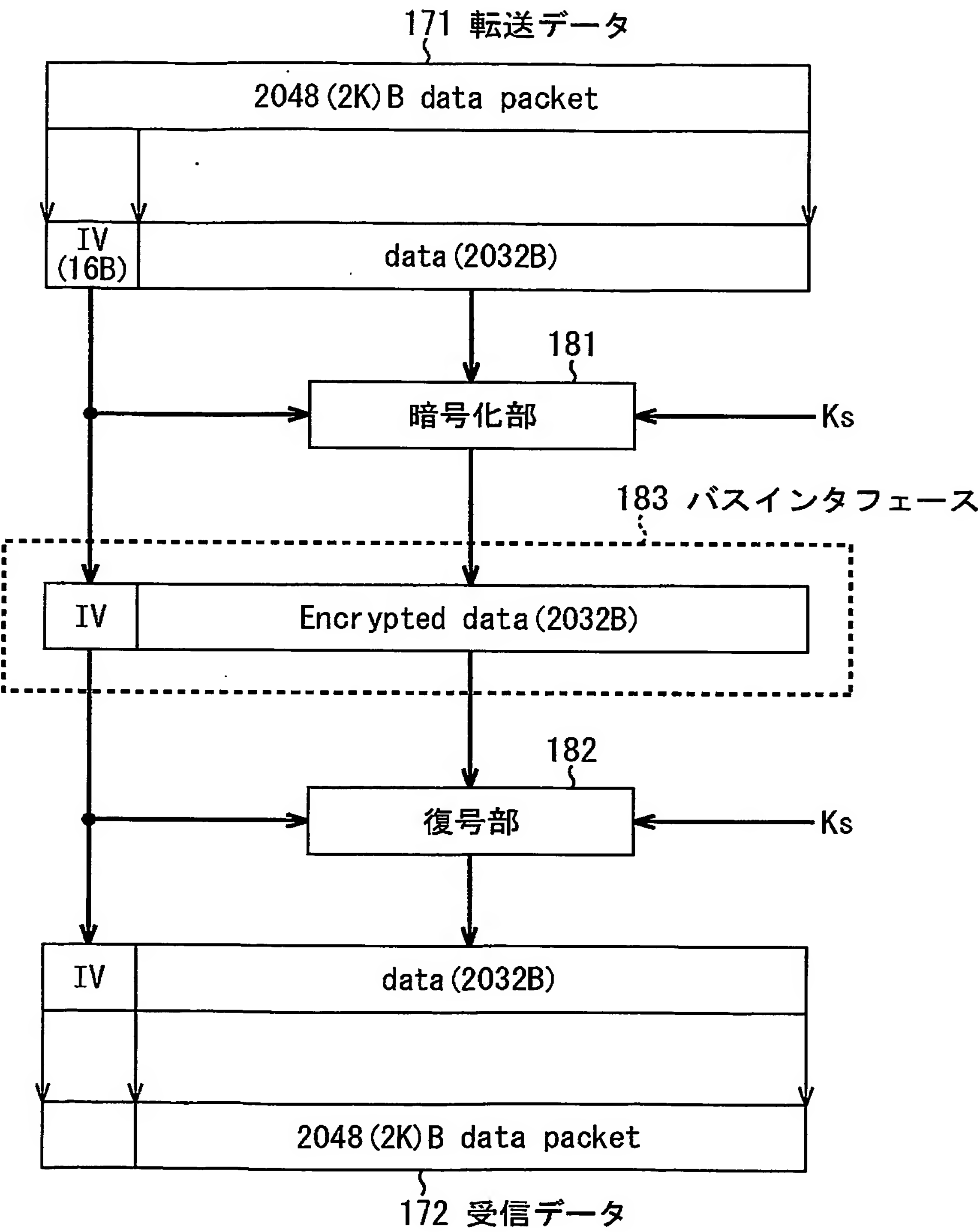
【図 6】
図6



【図 7】
図7

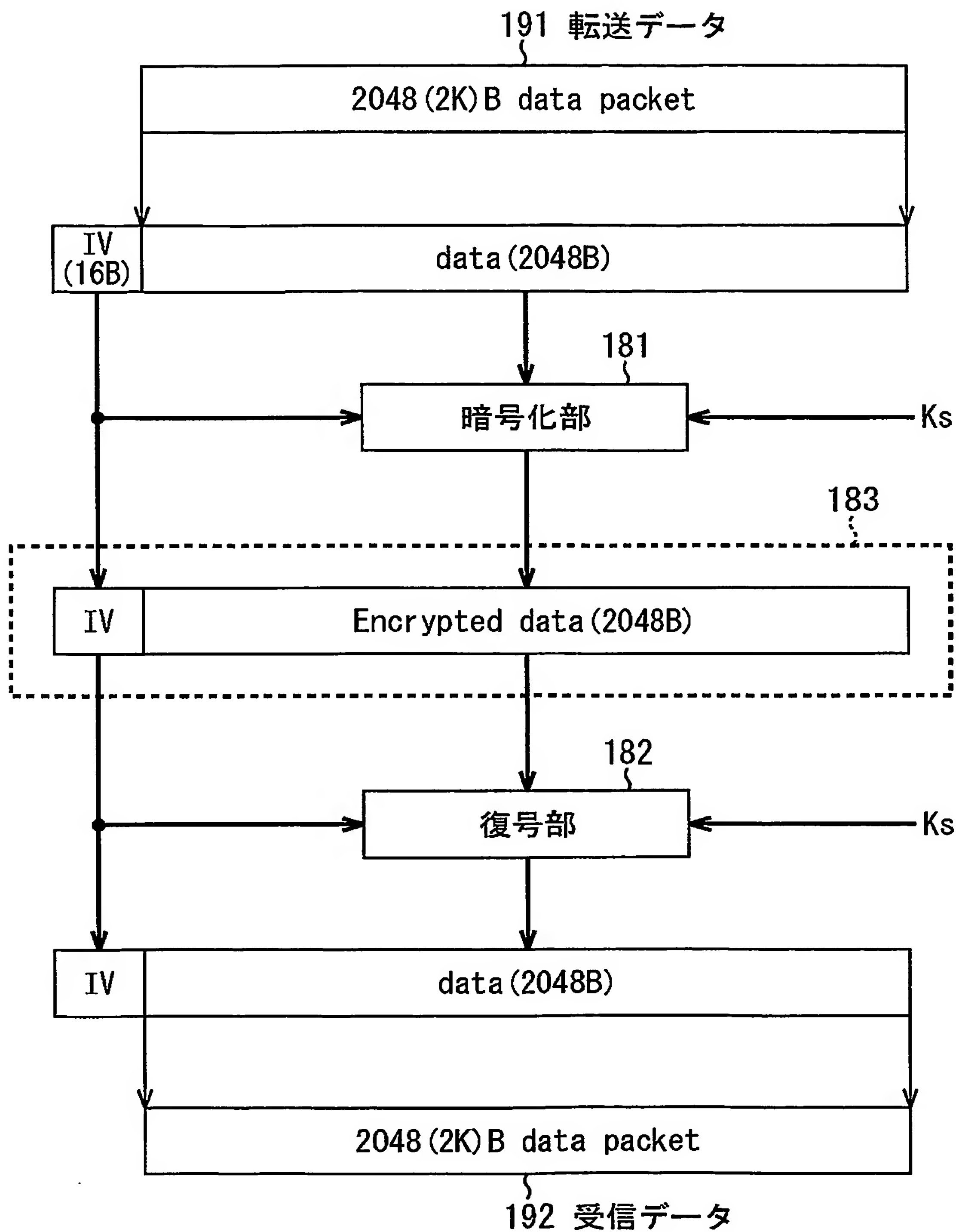


【図 8】
図8

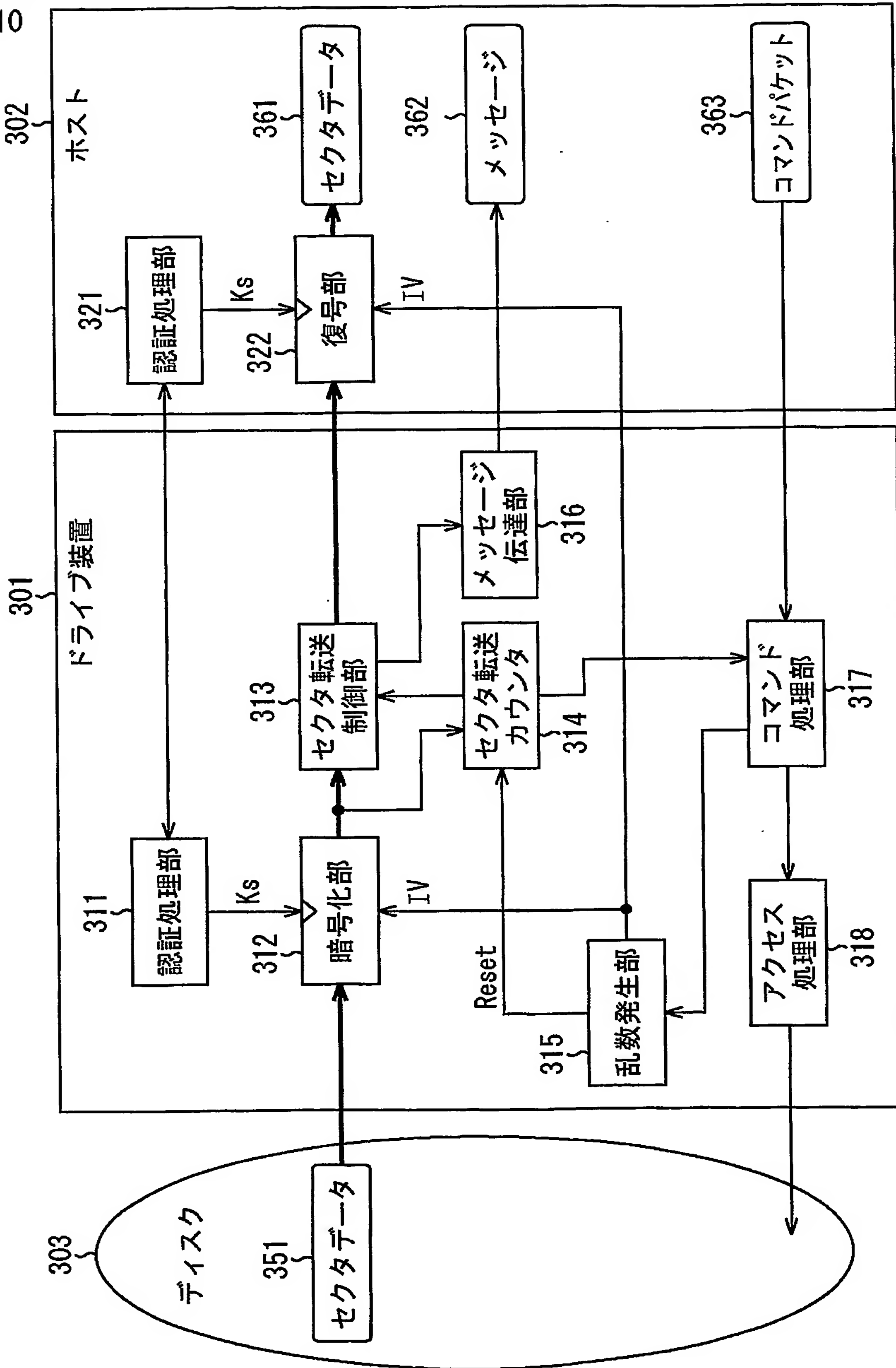


【図 9】

図9

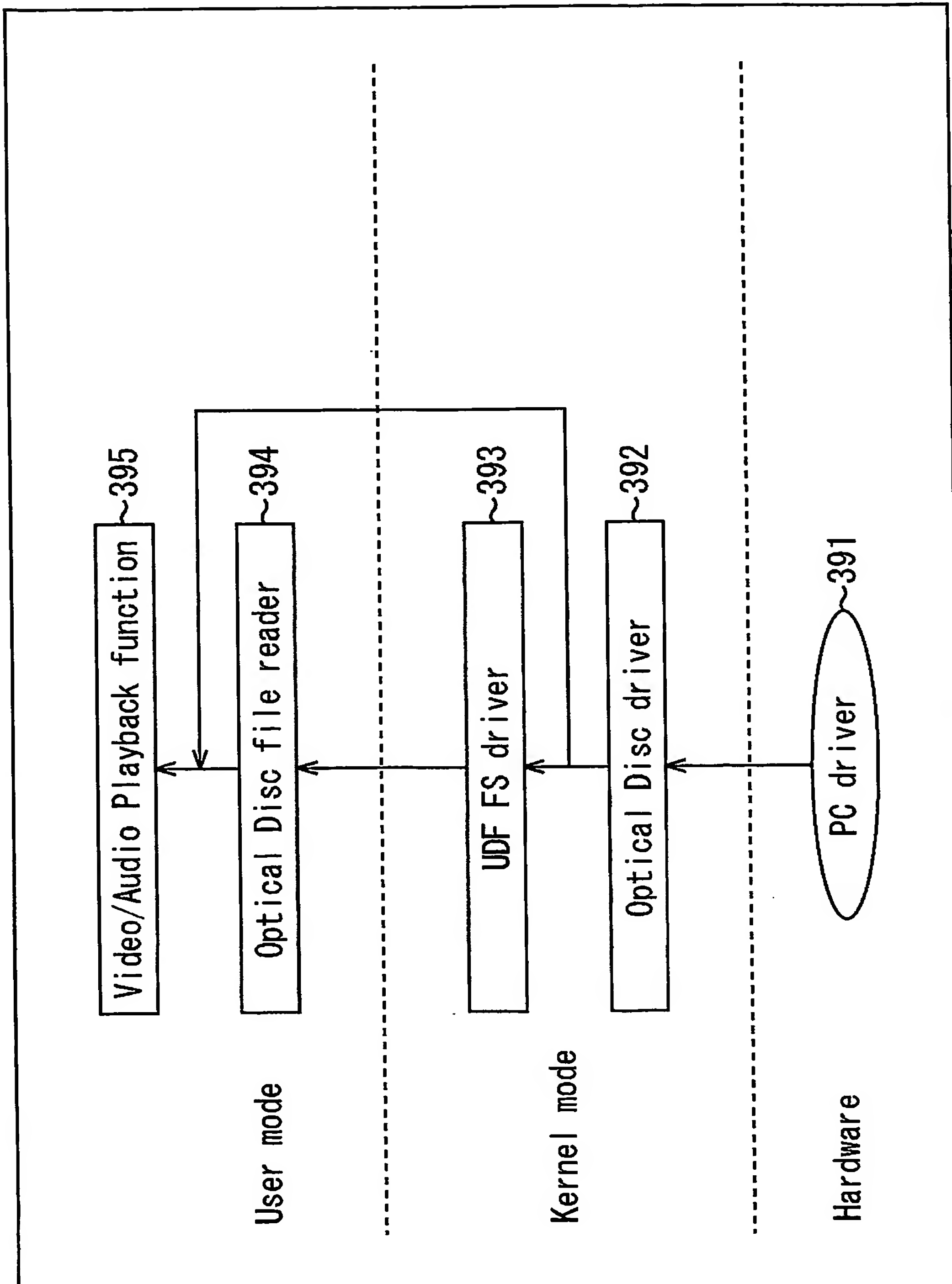


【図10】
図10

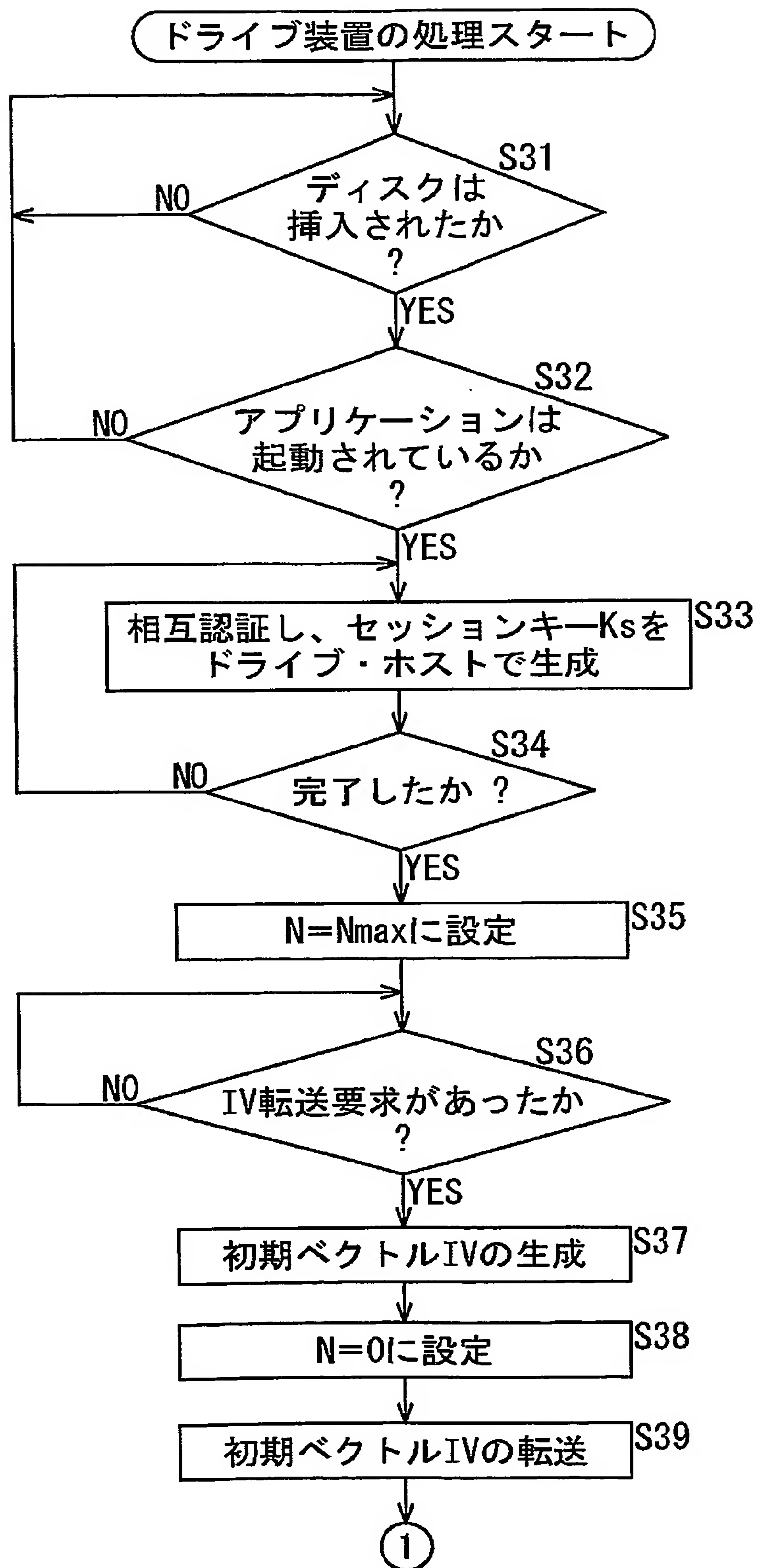


【図 1 1】

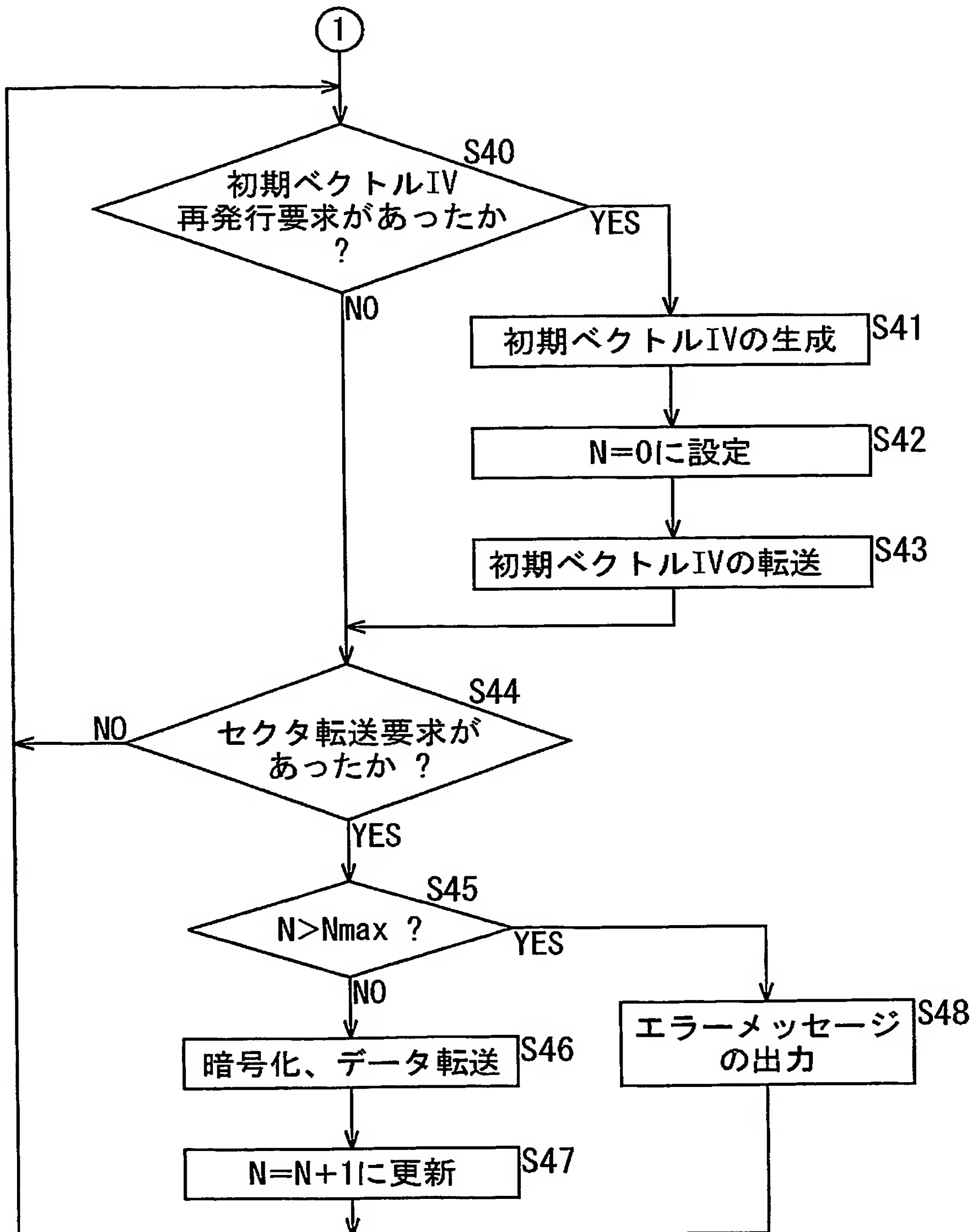
図11

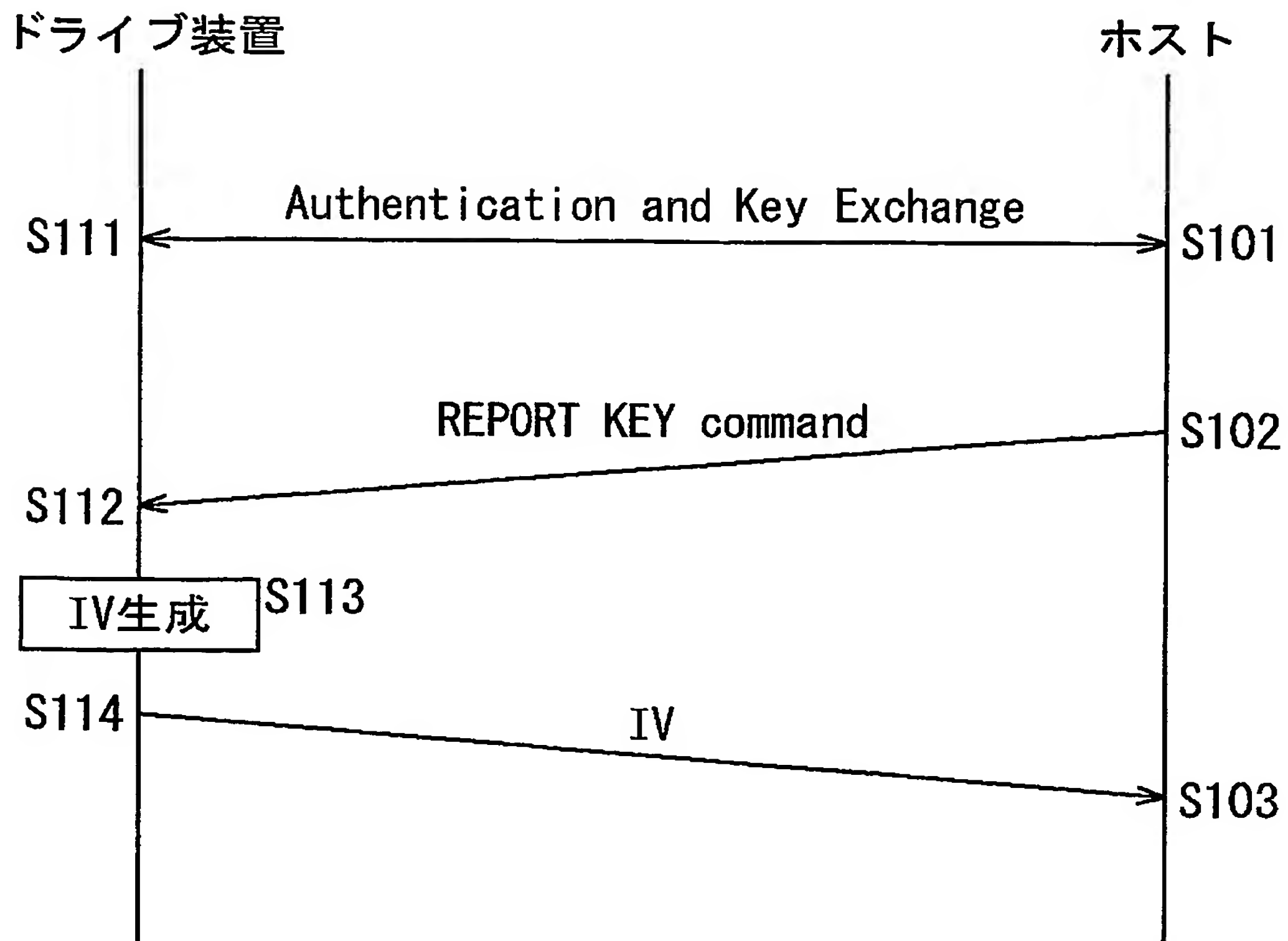
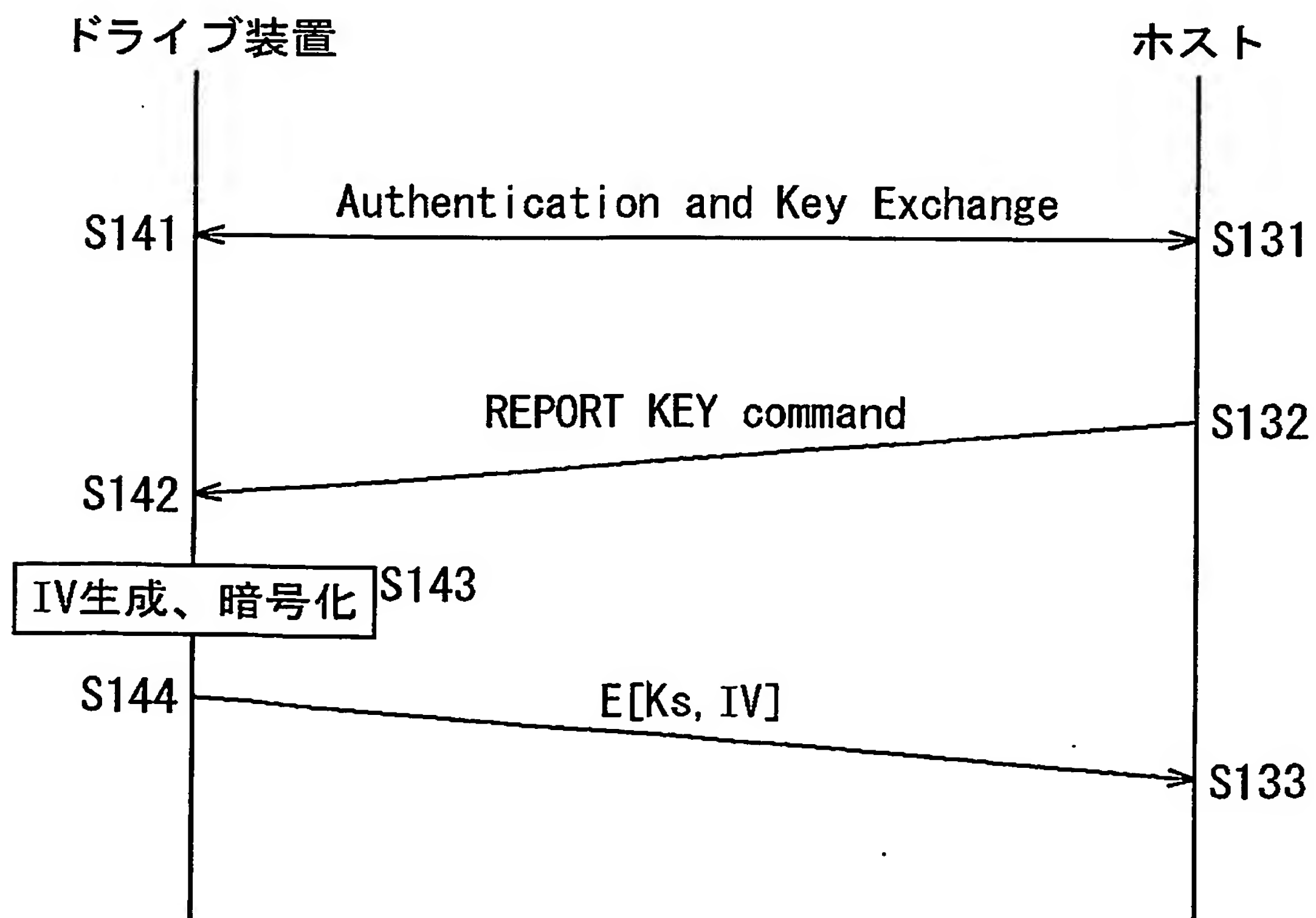


【図 12】

図12
(12-1)

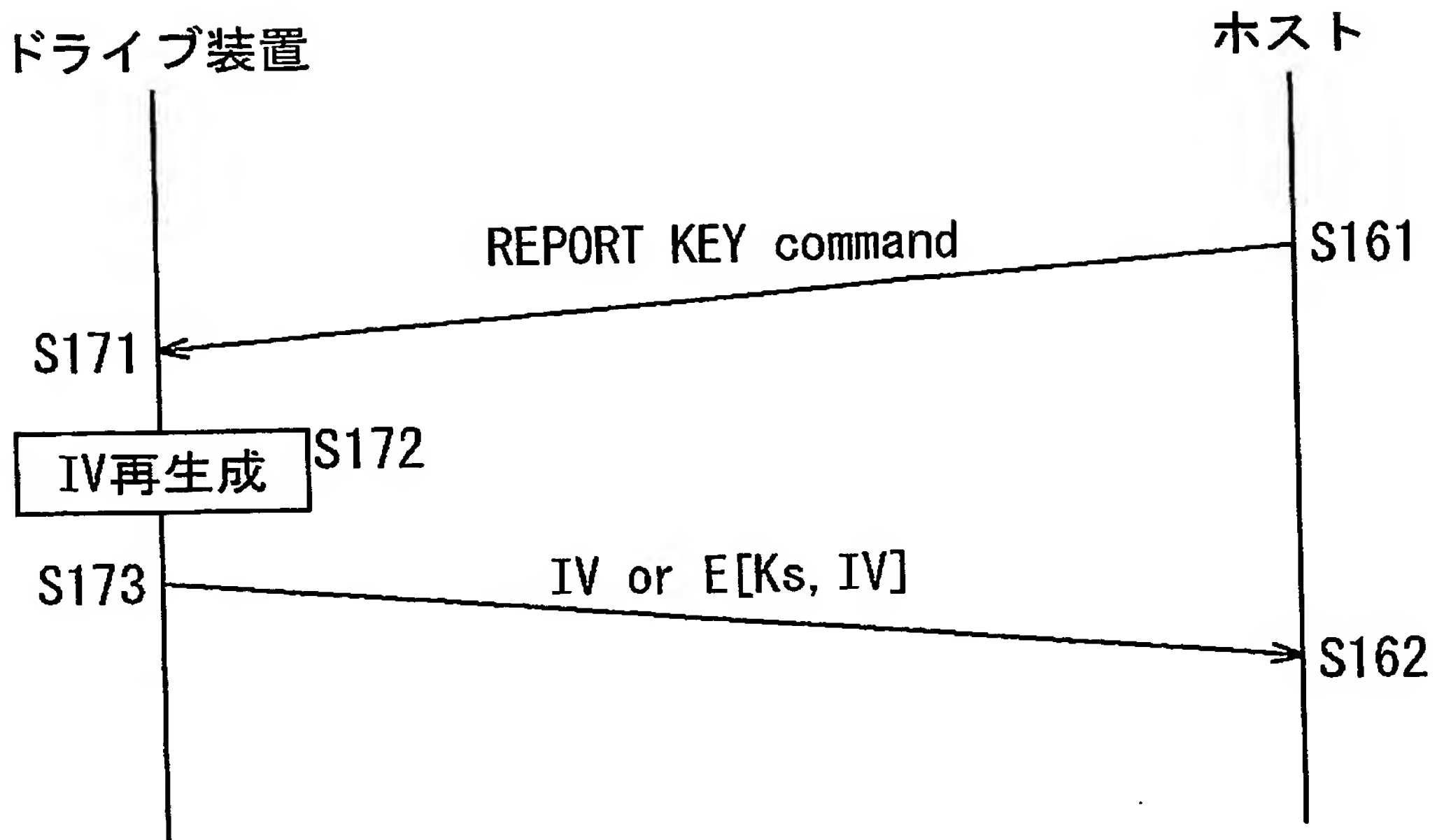
【図 13】

図13
(12-2)

【図 14】
図14【図 15】
図15

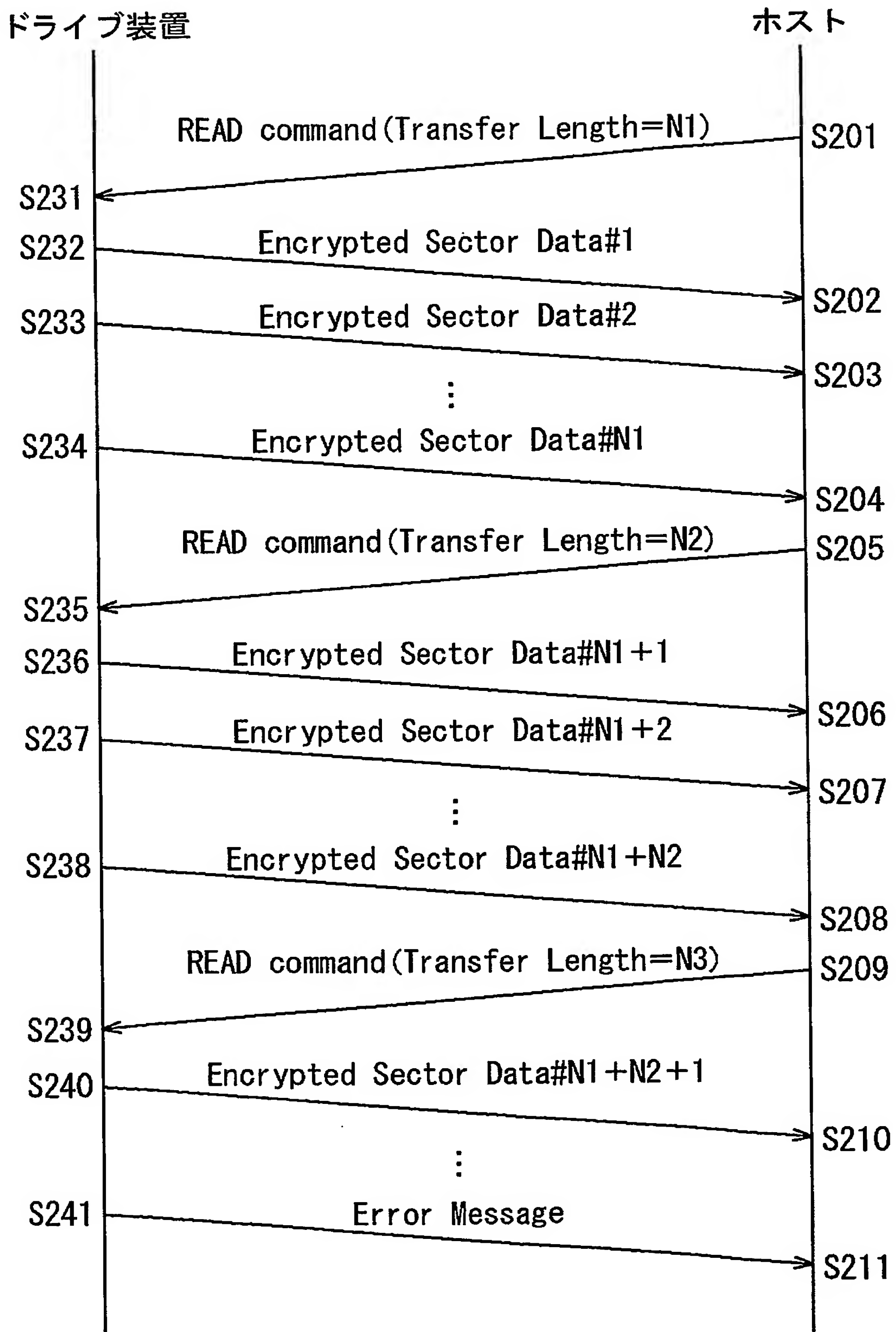
【図 1 6】

図16



【図 1 7】

図17

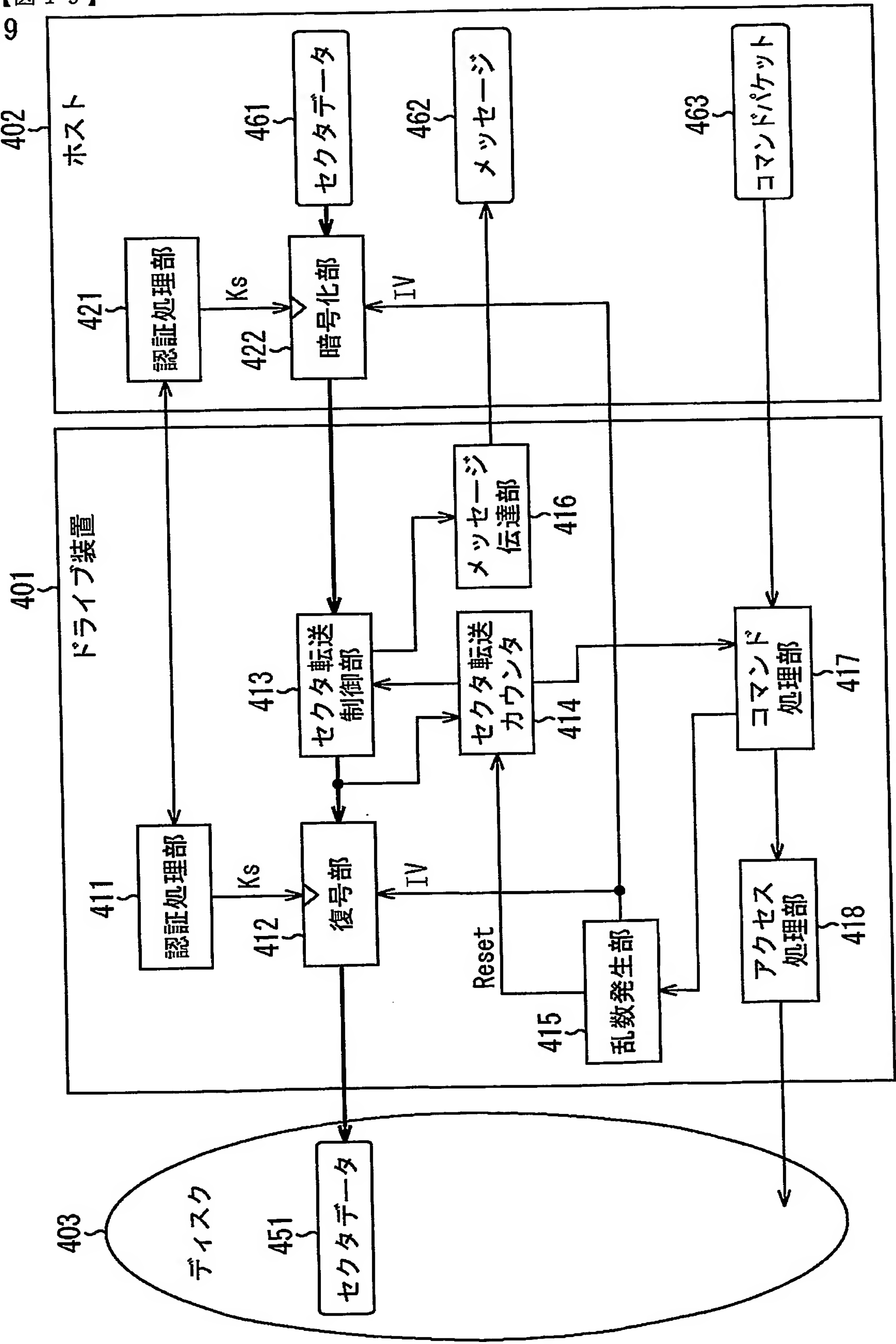


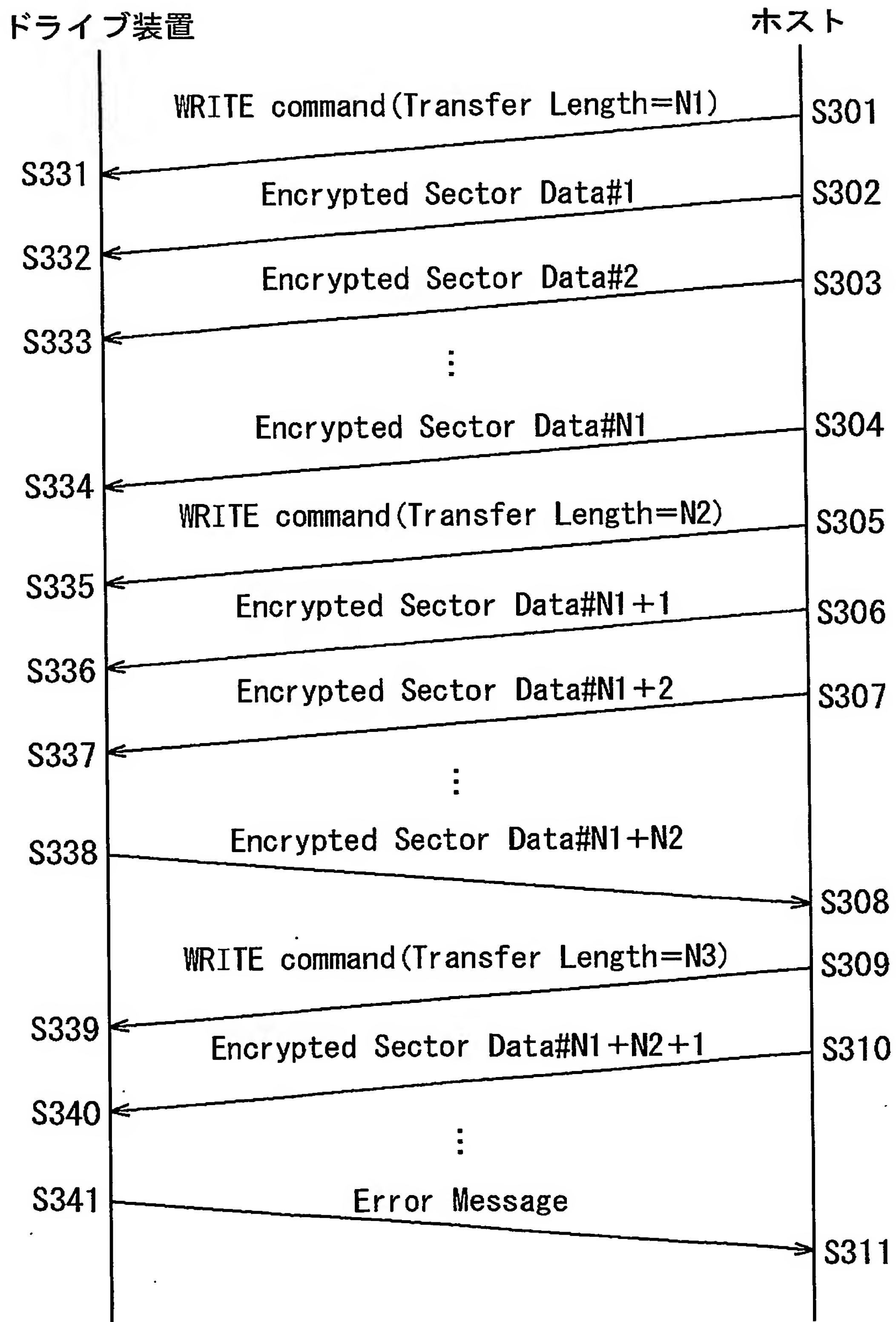
【図 1 8】
図18

Bit Byte	7	6	5	4	3	2	1	0
	363 {							
0	Operation Code							
1	LUN (Obsolete)				DPO (0)	FUA	Reserved	RelAdr
2	Logical Block Address (LSB)							
3								
4								
5								
6								
7	Transfer Length (LSB)							
8								
9								
10								
11	Streaming	Reserved						
	Vendor-Specific		Reserved		NACA		Flag	
							Link	

【図 19】

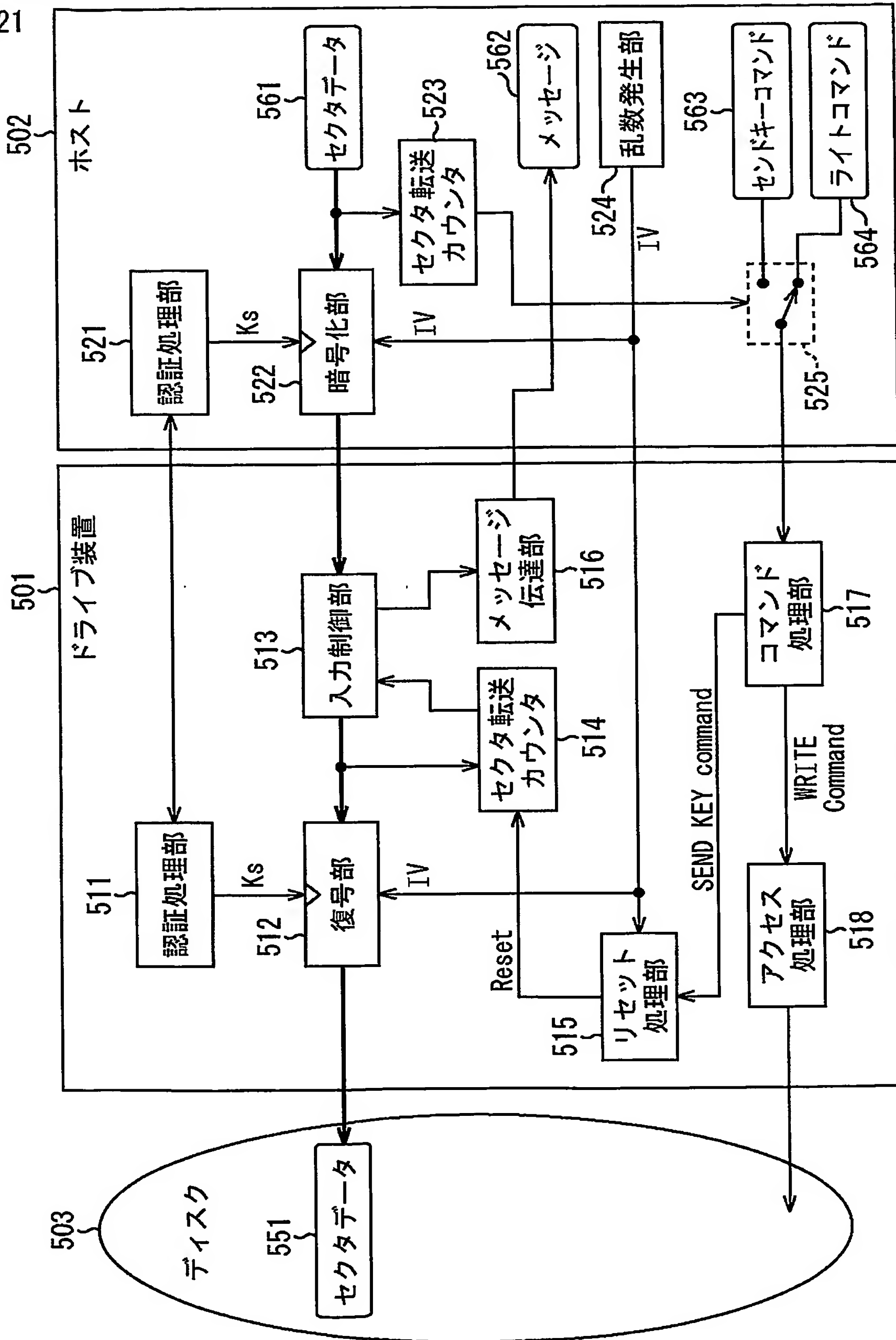
図 19



【図 20】
図20

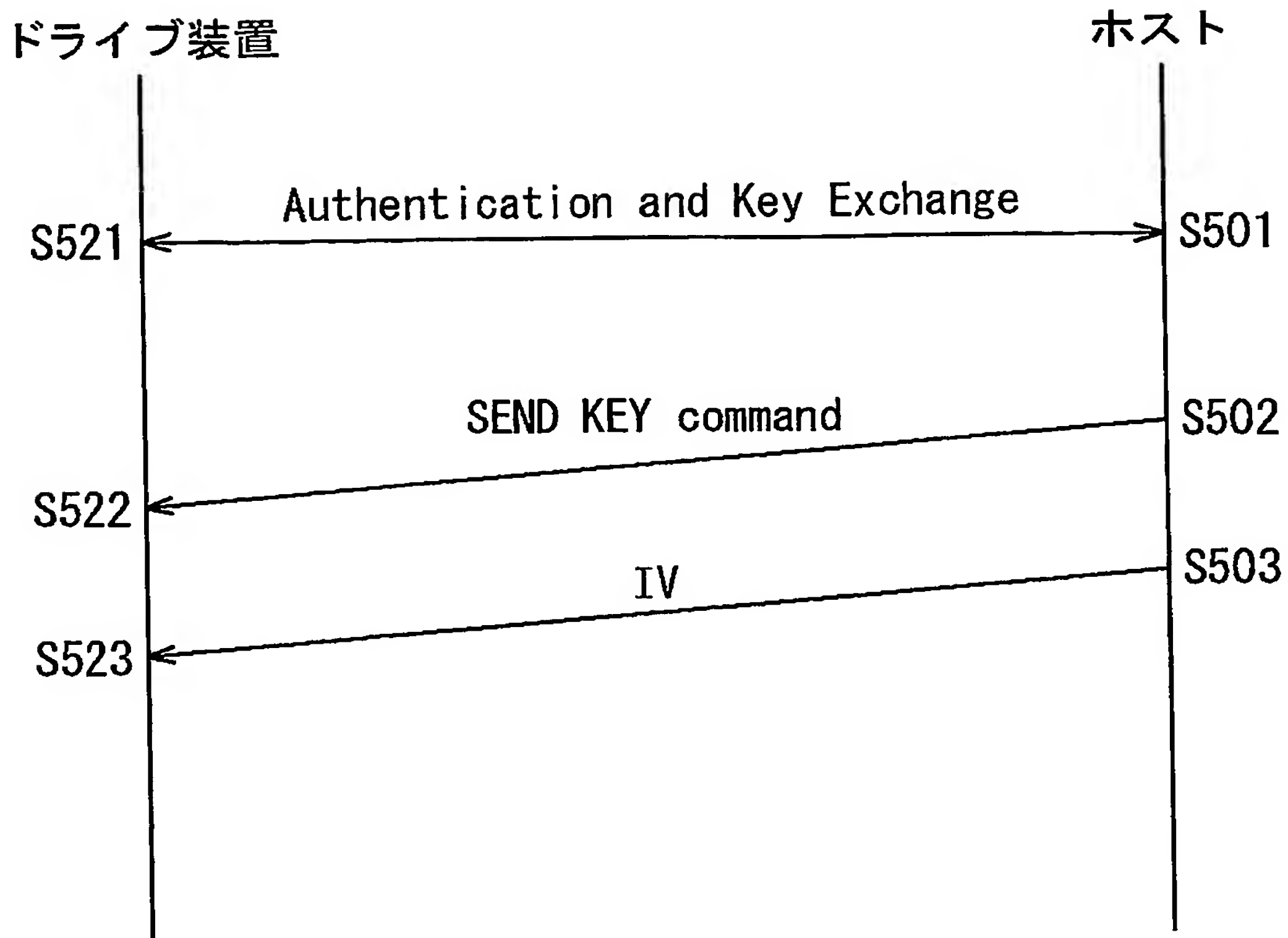
【図21】

図21



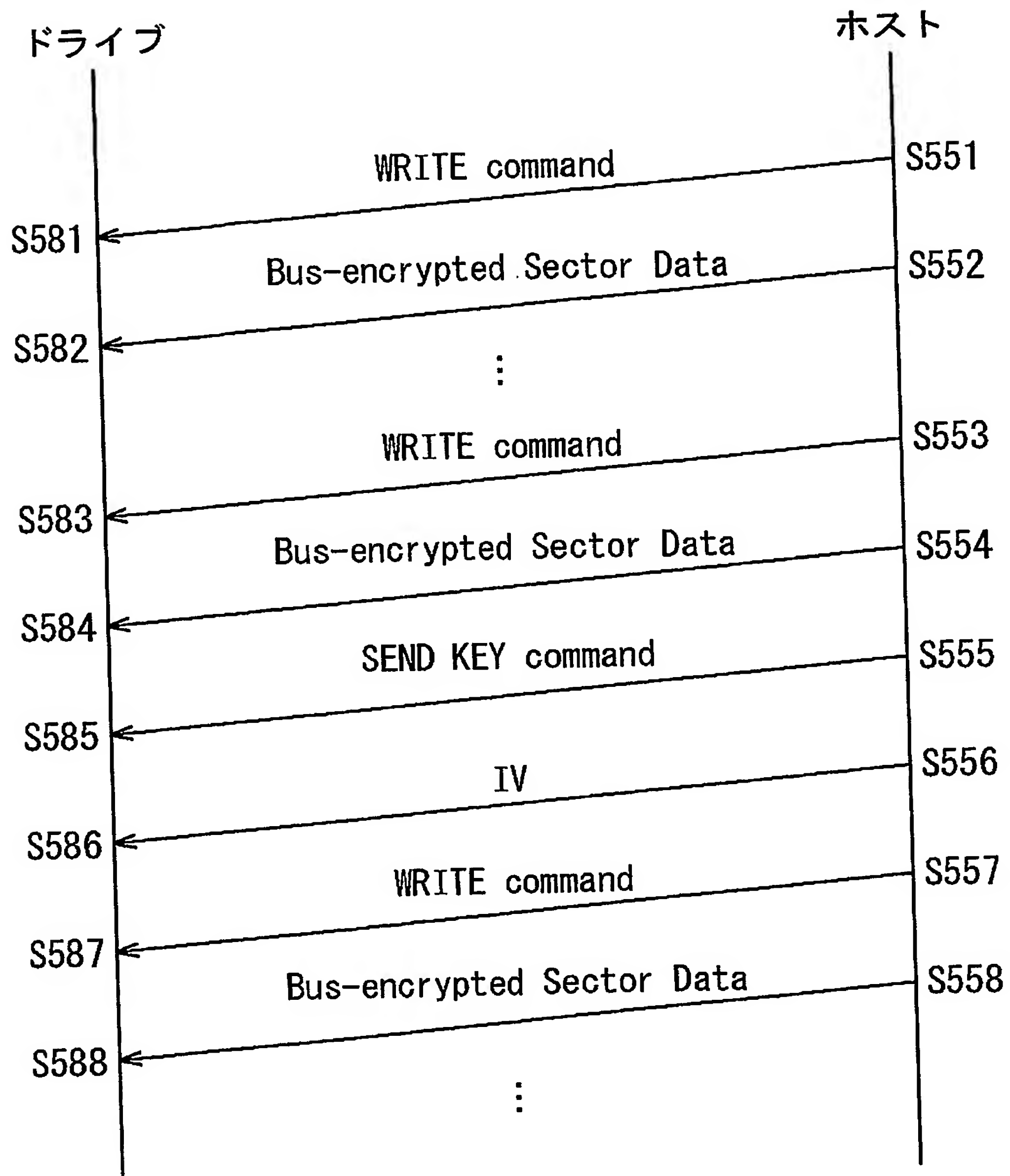
【図 2 2】

図22

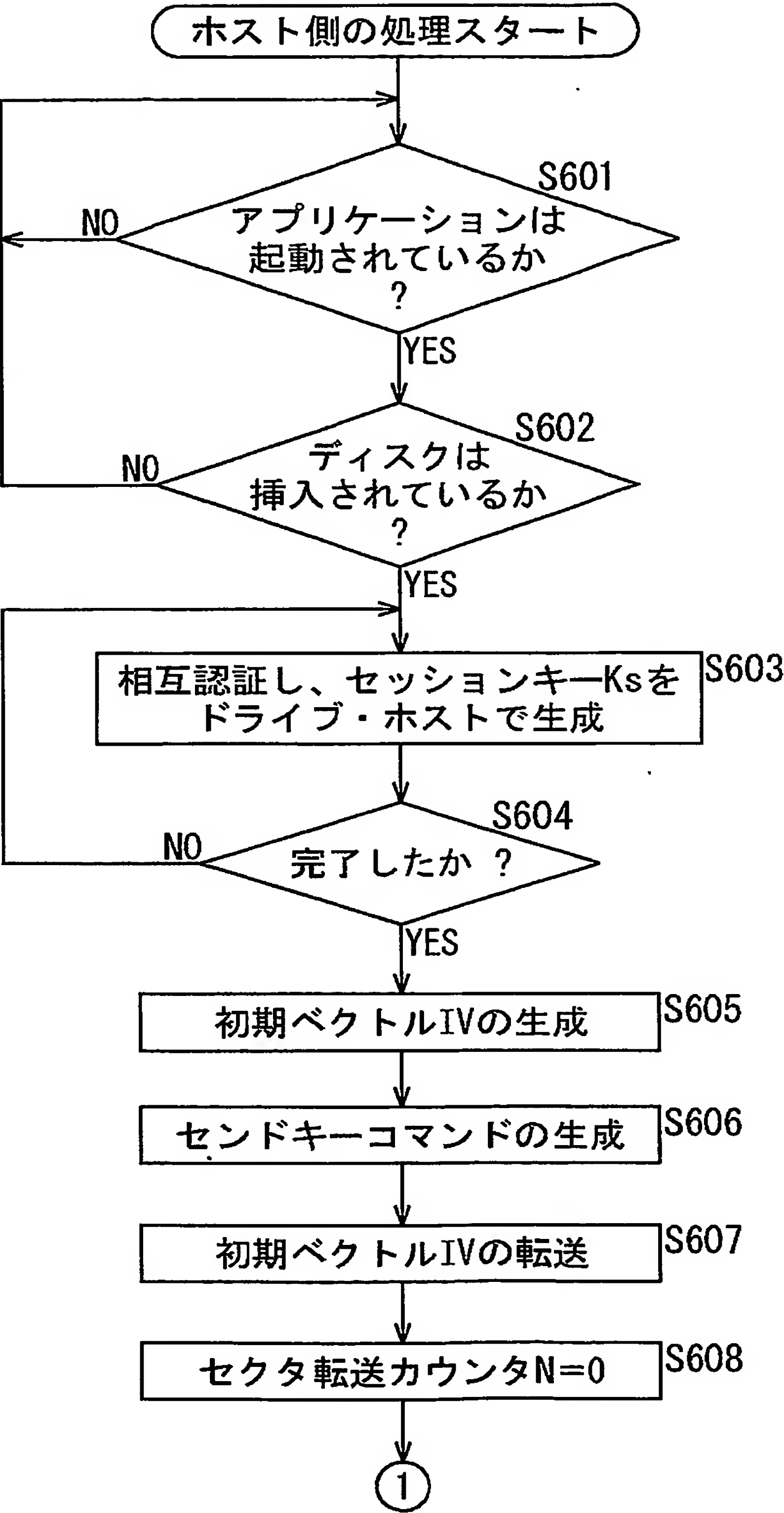


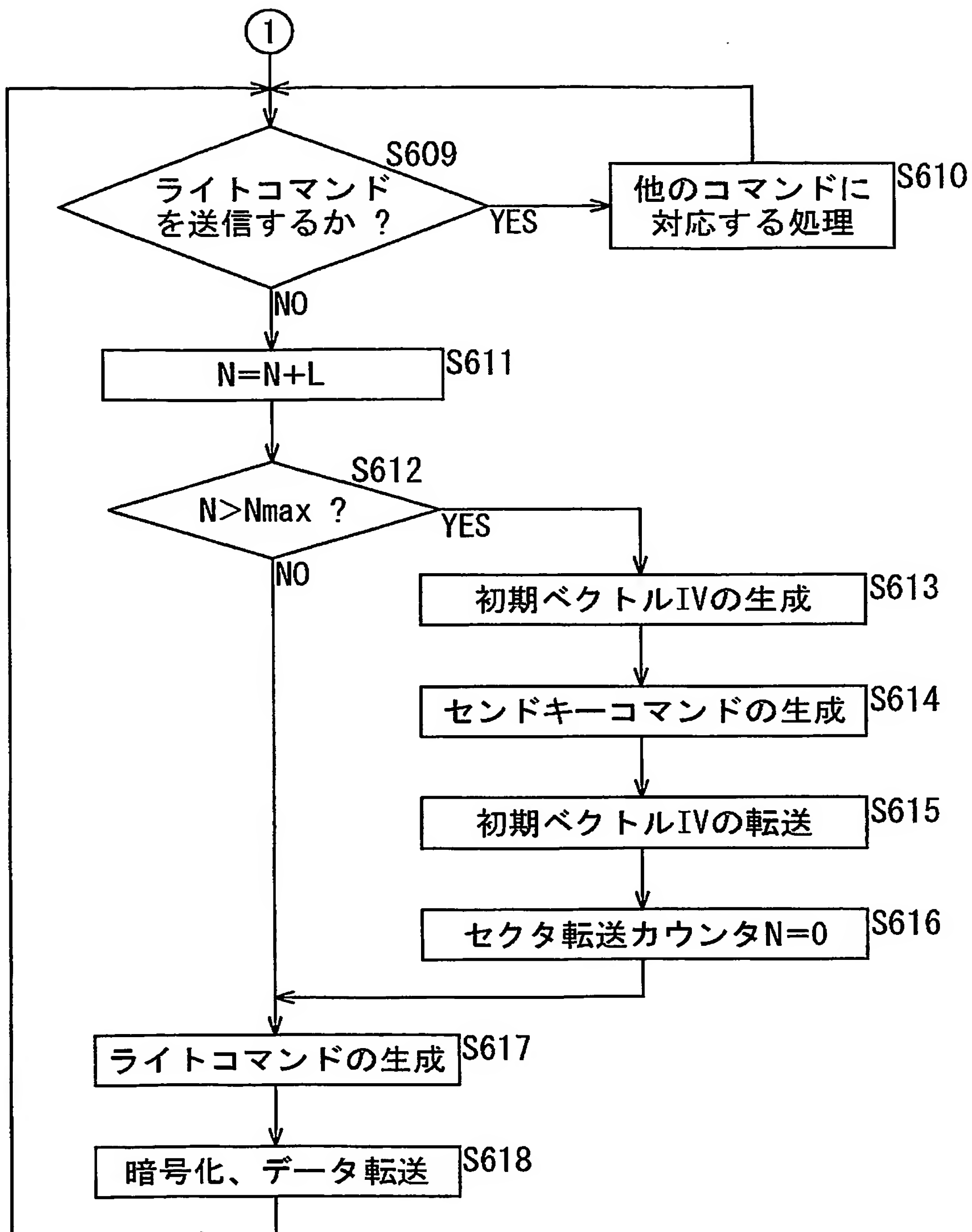
【図 23】

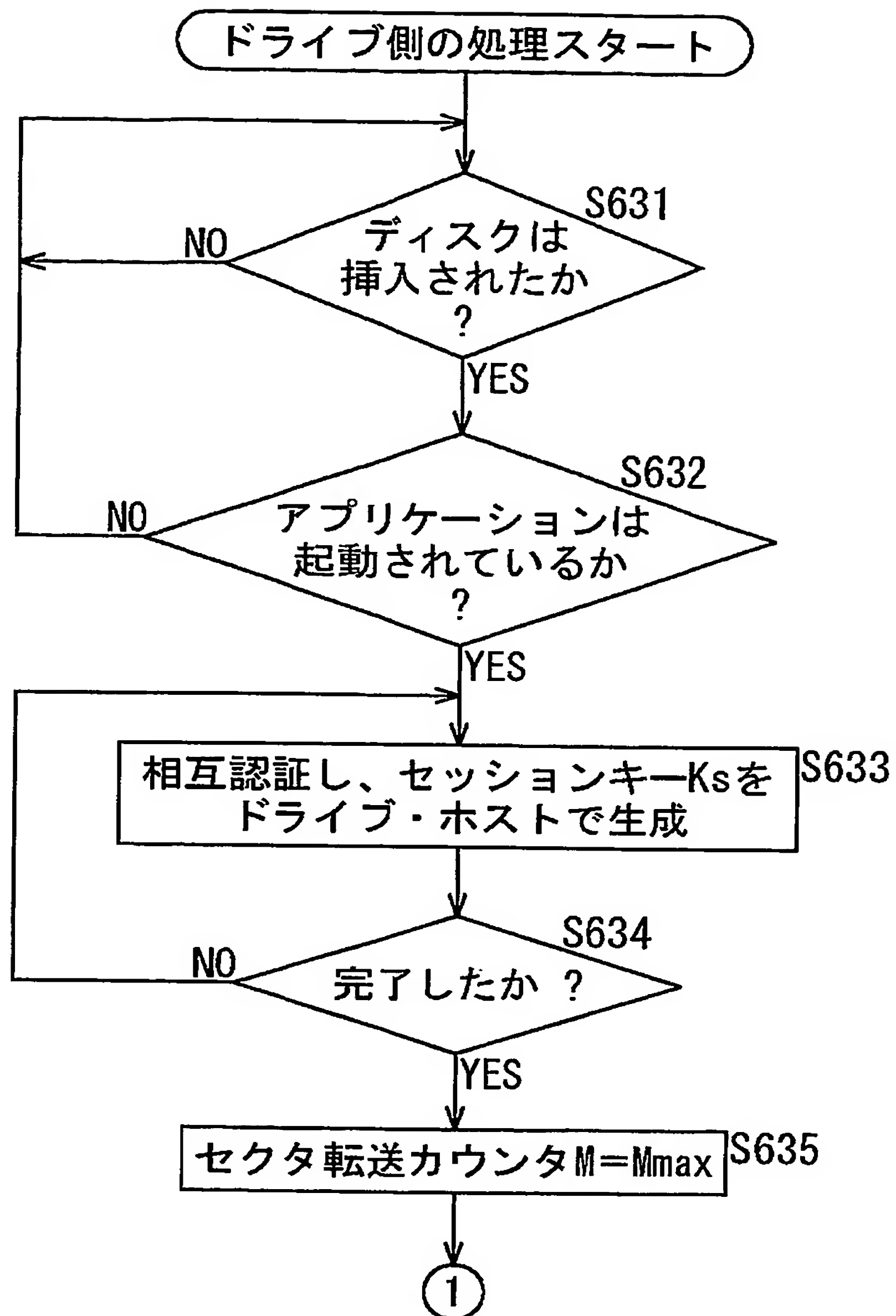
図23



【図 2 4】
図24

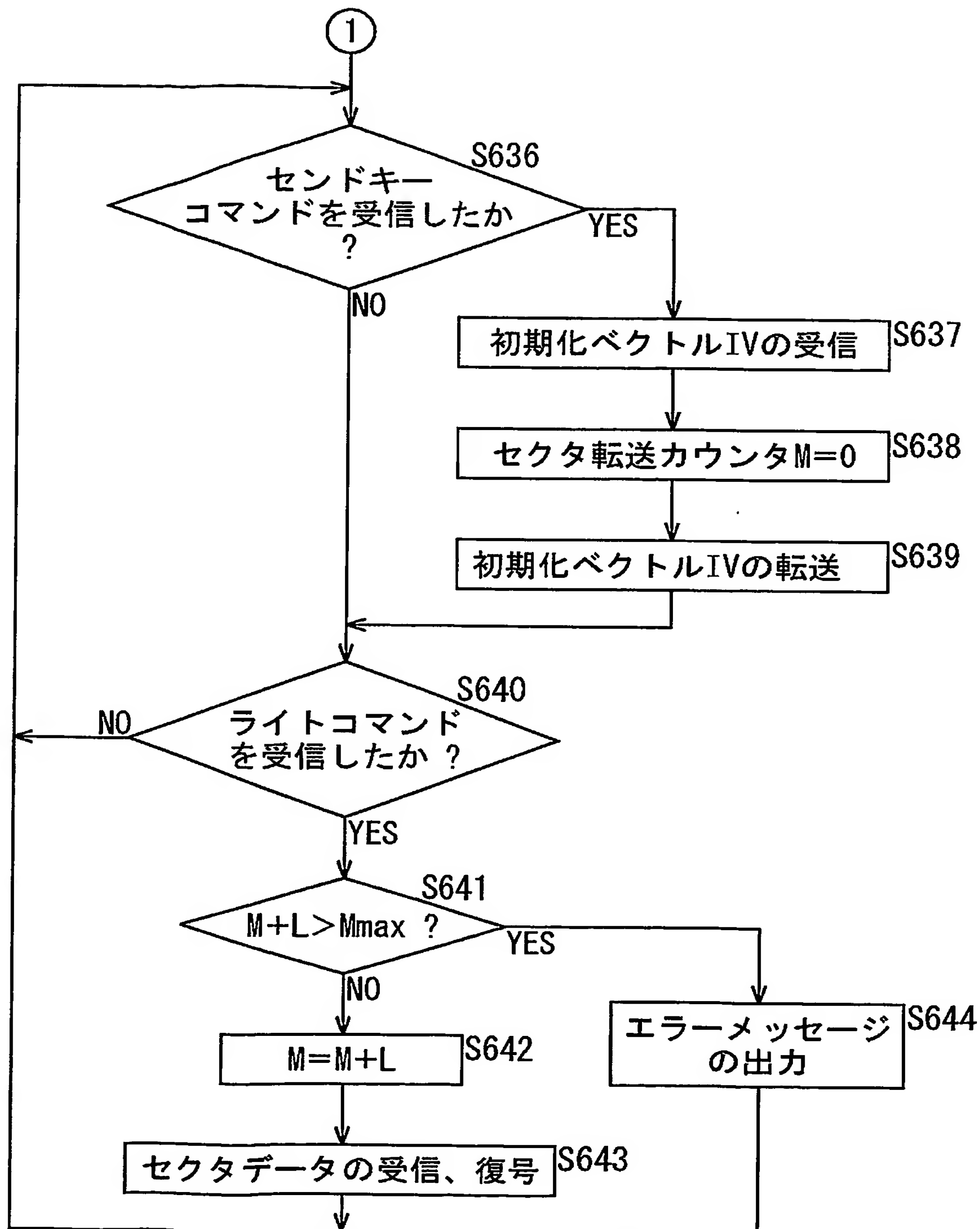


【図 25】
図25

【図 26】
図26

【図 27】

図27



【書類名】 要約書

【要約】

【課題】 データの授受をセキュリティを高めた状態で行えるようにする。

【解決手段】 ホストとドライブ装置は、所定のバスで接続されており、そのバスを介してデータの授受を行う。ホストは、ドライブ装置に対して、バス上を介して授受されるデータを暗号化および復号の際に用いられる初期ベクトル I V の発行の要求を定期的に行う。ドライブ装置は、要求があったとき、初期ベクトル I V を生成しホストに供給する。このような処理が定期的に行われなければ、ドライブ装置は、ホストに対するデータの出力を停止する。本発明は、記録媒体に記録されているデータを再生するドライブ装置を有するパーソナルコンピュータに適用することが可能である。

【選択図】 図 16

認定・付加情報

特許出願の番号	特願 2 0 0 4 - 1 2 2 5 2 4
受付番号	5 0 4 0 0 6 5 8 4 5 2
書類名	特許願
担当官	第八担当上席 0 0 9 7
作成日	平成 1 6 年 4 月 2 2 日

< 認定情報・付加情報 >

【特許出願人】	
【識別番号】	000002185
【住所又は居所】	東京都品川区北品川 6 丁目 7 番 3 5 号
【氏名又は名称】	ソニー株式会社
【代理人】	申請人
【識別番号】	100082131
【住所又は居所】	東京都新宿区西新宿 7 丁目 1 1 番 1 8 号 7 1 1 ビルディング 4 階 稲本国際特許事務所
【氏名又は名称】	稲本 義雄

特願 2 0 0 4 - 1 2 2 5 2 4 ,

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 2 1 8 5]

1. 変更年月日

1 9 9 0 年 8 月 3 0 日

[変更理由]

新規登録

住 所

東京都品川区北品川 6 丁目 7 番 3 5 号

氏 名

ソニー株式会社

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/000061

International filing date: 06 January 2005 (06.01.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-122524
Filing date: 19 April 2004 (19.04.2004)

Date of receipt at the International Bureau: 04 February 2005 (04.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse